Auteur : Lionel GUILLET
Expert en Management de la Sécurité de l'Information

LA GESTION DES EVENEMENTS ET DES INCIDENTS DE SECURITE NE PEUT PAS ETRE CONFONDUE AVEC LE PLAN DE CONTINUITE D'ACTIVITE

Ce n'est pas une inondation centennale, ce n'est pas une pandémie ou un incendie grave, non, ce n'est pas un sinistre majeur, c'est un incident de sécurité qui peut pourtant se révéler catastrophique pour une entreprise jusqu'à remettre en cause la poursuite de son activité.

C'est pourquoi l'une des premières actions à inscrire dans un Système de Management de la Sécurité de l'Information (S.M.S.I.), c'est la mise en place d'un dispositif d'alerte et de traitement des risques fonctionnels et opérationnels attachés aux activités.

C'est un processus de sécurité essentiel.

D'abord parce qu'il doit permettre d'intervenir vite et bien pour limiter les conséquences d'un incident et le prévenir par la suite.

Mais aussi, servi par une communication efficace sur son objet et ses résultats, il doit favoriser la sensibilisation de l'ensemble des utilisateurs du système d'information de l'entreprise aux objectifs poursuivis et aux risques encourus afin d'obtenir cette mobilisation collective indispensable à la protection de l'Information grâce à une meilleure connaissance des risques et des moyens de s'en préserver.

Par contre, pas n'importe quoi n'importe comment.

En effet, la démarche doit faire l'objet d'un dispositif et d'une procédure formellement définis et publiés à partir du respect de quelques fondamentaux sous peine, dans ce domaine aussi, de désordre et de confusion des rôles et des interventions.

C'est le propos de notre article rédigé en vérifiant (un peu) le cadre normatif, la norme Iso 27035, mais en proposant (surtout) à votre commentaire et vos contributions l'expression d'une expérience personnelle dans le domaine.

IL FAUT DEFINIR LE PERIMETRE DE CETTE ACTION

LE DISPOSITIF CONCERNE LES EVENEMENTS LIES A LA SECURITE DE L'INFORMATION, PAS SEULEMENT LES INCIDENTS, PAS SEULEMENT LES INCIDENTS … INFORMATIQUES

La démarche adresse les incidents, mais aussi les failles et les faiblesses du système d'information.

Évènement ou incident … la norme Iso 27000 distingue :

- les évènements, ce sont des failles de la politique de sécurité, des échecs dans les mesures, des situations non gérées …

- les incidents qui sont des … évènements (!) de nature à compromettre les activités de l'organisation et à menacer la sécurité de l'information.

Évènement ou incident, ce qu'il convient de retenir c'est que la norme ISO 27001, pour la mise en œuvre d'un Système de Management de la Sécurité de l'Information, et la norme 27035, dédiée à notre sujet, confondent les deux notions pour exprimer leurs recommandations.

C'est pourquoi, à notre sens, le terme "évènement" convient mieux que le terme restrictif "incident" pour désigner ce processus de large périmètre qu'il faut définir et formaliser.

En effet, il traite, sauf mis à part d'un domaine objet d'une action particulière, **l'ensemble des évènements liés à la Sécurité de l'Information dans tous les domaines listés à la norme Iso 27001** (Cf. article "Pour inscrire le PCA dans la durée" page 4, sur BCP-Expert) .

… une défaillance dans la protection de données à caractère personnel, une vulnérabilité d'accès physique ... en feront partie.

Naturellement, les incidents informatiques sont concernés en tout premier lieu, mais, à la condition de souscrire aux critères d'évaluation en termes de portée, d'impact, de durée (par exemple, la désactivation d'un anti-virus sur un poste de travail, la panne d'un disque dur n'entreront pas dans ce cadre).

TOUTES LES SITUATIONS POTENTIELLEMENT DANGEREUSES OU NE SERAIENT-CE QUE SUSPECTES DE L'ETRE

Failles, vulnérabilités, … nous l'avons dit, **IL PEUT S'AGIR DE SITUATIONS SANS CONSEQUENCES REELLES IMMEDIATES** mais qui présentent des risques pour l'Information dans son intégrité, sa disponibilité et sa confidentialité.

Et plus, dans un contexte où les menaces se font de plus "professionnelles", il ne faut pas s'épargner d'inviter les utilisateurs du système d'information de l'entreprise à signaler également **LES SITUATIONS** qui leur paraissent **SUSPECTES**.

Dans ces conditions, évènements ou incidents, réels ou potentiels, voire suspectés … la notion doit faire l'objet d'une définition précise dans la procédure afin de limiter les interprétations erronées et les dérives d'usage.

Egalement, la publication d'une liste générique des menaces et des vulnérabilités, de leurs causes et de leur origine, ne peut qu'aider les utilisateurs du S.I. dans un rôle majeur, la détection et la description de premier niveau de l'évènement.

Il y en a d'autres, mais, la base de connaissances de la méthode EBIOS publiée par l'ANSSI peut aider dans l'élaboration de ce référentiel, tel quel ou adapté aux spécificités d'activité de l'entreprise[1].

Dernière recommandation, afin d'éviter la multiplication des alertes intempestives, il est utile de proposer aux utilisateurs du système d'information la possibilité de joindre la personne ou le service habilité à recevoir le signalement en cas de doute sur l'opportunité de déclencher le dispositif.

[1] Par commodité, le vocable "entreprise" désignera dans l'article toutes les formes d'organisation intéressées par le sujet, les unités économiques du secteur privé, les administrations et services publics, les associations …

TOUTES LES ENTREPRISES DE TOUTE TAILLE ET DE TOUTE NATURE SONT INTERESSEES

Les risques et les besoins de Sécurité ne sont pas liés à la taille de l'entreprise.

Ils dépendent des exigences d'activité, du patrimoine informationnel et des enjeux métiers mis en évidence à l'analyse.

Petite, moyenne ou grande, l'entreprise doit protéger son système d'information en mettant en place les dispositifs nécessaires à cet effet, notamment un dispositif d'alerte et de suivi des évènements de nature à mettre en danger son système d'information.[2]

Il est vrai que les petites entreprises sont confrontées à des limites de moyens.

Il n'en demeure pas moins qu'elles ne sont pas épargnées par les risques attachés à leurs activités. Il leur est donc plus que recommandé de mettre en place, elles aussi, dans leur contexte, des mesures de détection / correction des évènements de sécurité basées sur les principes publiés et présentés dans cet article.

IL FAUT SE PREPARER

DETECTER ET ELIMINER UN RISQUE LE PLUS RAPIDEMENT POSSIBLE, LA DEMARCHE VAUT BIEN UN PROCESSUS

Un simple listage des principaux avantages d'une approche organisée de la gestion des évènements de sécurité suffit pour mettre en évidence les avantages de cette gestion :

- Favoriser l'efficacité et l'efficience d'interventions
- Limiter les conséquences des dysfonctionnements du S.I. sur les activités
- Identifier et mettre en œuvre des actions correctives et préventives
- Faciliter le diagnostic par la constitution d'une base d'incidents et de solutions de référence
- Disposer d'exemples concrets de risques pour communiquer et sensibiliser tous les personnels
- Conserver la trace des interventions afin de disposer de preuves si nécessaire[3]
- Valoriser la Politique de Sécurité de l'Information de l'entreprise, sa mise en œuvre, mais aussi, permettre sa mise à jour à partir de cette approche par les risques
- Démontrer, pour la Direction, l'attention portée à la préservation des biens et des activités de l'entreprise tant en interne qu'auprès de partenaires et des clients

…

Un dispositif de gestion des incidents au point doit donc aboutir à une amélioration du niveau général de Sécurité de l'Information de l'organisation.

---

[2] Un rappel essentiel. Le système d'information est encore trop souvent confondu avec le système informatique qui n'en est qu'un composant, un composant prééminent, certes, mais … Le système d'information désigne l'ensemble des moyens nécessaires à la collecte, au traitement, à la conservation de l'Information (organisation, ressources humaines, réglementations, moyens matériels, réseau …)

[3] La preuve, la recherche en responsabilité, pour être établie, doit satisfaire des conditions strictes de collecte, de conservation et de production. La formalisation des conditions à satisfaire relève de compétences juridiques.

QUI DIT PROCESSUS, DIT PROCEDURE ET ORGANISATION POUR ETRE PRET LE MOMENT VENU

La formule est connue, mais il faut la rappeler. La question qui se pose n'est pas, "Que ferai-je s'il arrive un incident de sécurité ?" mais plutôt, "Que ferai-je quand arrivera un incident de sécurité?

La démarche ne s'improvise pas en situation de difficulté, en effet.

C'est une évidence, mais il convient de le rappeler, car, encore trop souvent, même si la prise de conscience progresse, les entreprises ne se sentent pas directement exposées aux menaces et aux risques qui, pourtant, s'accentuent avec l'évolution des moyens d'accès, de traitement et de communication de l'Information et de leurs usages.

Il faut donc préparer, organiser, prévoir les moyens à mettre en œuvre.

Pour cela **UNE PROCEDURE** doit décrire les différentes étapes de gestion, l'organisation mise en place, les intervenants, les interventions et leurs modalités.

Voyons tout cela d'un peu plus près …

LES ETAPES POUR FAIRE LE TOUR DE LA QUESTION

LA DETECTION ET L'ALERTE – L'AFFAIRE DE TOUS LES UTILISATEURS DU SYSTEME D'INFORMATION

Essentiel. La performance du système repose sur **LA VIGILANCE ET LA REACTIVITE_DE L'ENSEMBLE DES PERSONNELS** afin de détecter et de traiter les incidents/évènements le plus rapidement possible.

C'est d'autant plus vrai aujourd'hui qu'avec le développement de la cybercriminalité, de nouvelles menaces sont apparues.

Les attaques se font de plus en plus souvent discrètes, ciblées, très élaborées, difficilement détectables. Par exemple, c'est le cas des "attaques persistantes avancées" qui utilisent des méthodes de sollicitations personnalisées, des méthodes d'ingénierie sociale, pour s'introduire, et se maintenir, dans un système d'information précisément identifié.

En plus, elles ont régulièrement un temps d'avance sur les solutions techniques de protection.

Conséquence, face à cette réalité, le recoupement de **SIGNALEMENTS** spontanés **D'EVENEMENTS SUSPECTS** ne peut que donner de meilleures chances d'identifier les attaques de ce type.

(Il ne faut pas perdre de vue que des affaires de vol d'informations comme celles qui se sont produites au ministère des finances, début 2011, et auprès de l'Élysée, mi 2012, ont été détectées par des utilisateurs qui ont alerté sur des mouvements suspects de courrier électronique).

Pas de doute, **LA SENSIBILISATION** des personnels, **DE TOUS LES PERSONNELS,** à la démarche et à ses enjeux est essentielle à son efficacité. Elle sera utilement complétée par **UNE INITIATION CONCRETE AUX RISQUES** les plus courants pour les utilisateurs (reconnaître un message douteux, un fichier suspect, utiliser une clé USB avec précaution, signaler une alerte virale …)

MAIS AUSSI, il faut impliquer dans cette démarche **TOUS LES UTILISATEURS DU SYSTEME D'INFORMATION DE L'ENTREPRISE**, prestataires, fournisseurs, partenaires, clients … en leur communiquant les informations nécessaires en temps utile et sous les formes adaptées.

Donc, pour alerter, il faut avoir compris les enjeux, mais, il faut avoir aussi connaissance de la procédure et des modalités de signalement mis en place.

POUR ALERTER, UN ECRIT ELECTRONIQUE STRUCTURE, UN FORMULAIRE

Ils peuvent précéder dans l'urgence son envoi, mais, plutôt que le téléphone, la messagerie, la remontée hiérarchique des informations, … **UN SUPPORT ELECTRONIQUE DE DESCRIPTION DE SITUATION** comprenant les premières informations indispensables, un support, **COMMODEMENT ACCESSIBLE A TOUS LES UTILISATEURS DU SECURITE DE L'INFORMATION,** fait parfaitement l'affaire.

Le formulaire électronique présente l'avantage, en effet, de faciliter la communication, la mise en partage, l'enrichissement et la conservation d'informations structurées pour une utilisation ultérieure.

Son envoi **DANS LES MEILLEURS DELAIS** bien évidemment, sera effectué **DANS LE CADRE D'UN CIRCUIT DE TRANSMISSION FORMELLEMENT ETABLIE**. (Un modèle de document vous est proposé en annexe).

Et ce support, même adressé pour information à des autorités hiérarchiques concernées, a un seul destinataire pour action.

UNE ORGANISATION POUR L'EVALUATION, LE SUIVI, LE DIAGNOSTIC ET LE TRAITEMENT

UN POINT D'ENTREE UNIQUE DE TOUTES LES ALERTES POUR EVALUATION, VALIDATION ET CARACTERISATION DE L'INCIDENT / EVENEMENT DE SECURITE.

Il s'agit d'un personnel, ou d'une structure, dont le rôle essentiel est d'évaluer la nature et la portée des évènements signalés et leurs conséquences effectives et potentielles.

C'est ce point d'entrée qui vérifie s'il s'agit bien d'un incident à inscrire dans le dispositif de gestion spécifique prévu, qui va informer les Autorités intéressées, internes et externes, le cas échéant, et organiser la cellule de gestion qui sera chargée de traiter l'affaire.

Service ou expert, sa spécialité, c'est d'être … généraliste de la Sécurité de l'Information doté des connaissances et des capacités requises pour la conduite générale des démarches. C'est un manager, le coordonnateur et l'évaluateur nécessaire pour des interventions le plus souvent interdisciplinaires et transversales.

L'architecte référent en Sécurité des systèmes d'information défini par l'Agence Nationale à la Sécurité des Systèmes d'information (A.N.S.S.I.) a le bon profil pour ce rôle d'ailleurs évoqué dans le référentiel emploi correspondant.

Ce n'est surtout pas un spécialiste d'un domaine précis, pas plus en informatique qu'un autre. Ces spécialistes nous les retrouvons dans la Cellule de Traitement des Evènements de Sécurité

UNE CELLULE DE TRAITEMENT DES EVENEMENTS DE SECURITE POUR UNE APPROCHE COLLEGIALE DU DIAGNOSTIC ET DU TRAITEMENT

Une cellule de veille et d'intervention, la Cellule de Traitement des Evènement de Sécurité est en place pour un travail en mode collaboratif et des points de situation réguliers avec le gestionnaire chargé du suivi, le point d'entrée des alertes.

La liste DES SPECIALISTES qui LA COMPOSENT est annexée à la procédure publiée, et tenue à jour régulièrement.

Tous les domaines prévus à la norme ISO 27001 sont représentés.

Les membres de cette cellule sont formés aux enjeux attachés au rôle qui leur est confié afin de pouvoir compter sur leur engagement le moment venu.

La composition de l'équipe d'intervention lors d'une alerte est à dimension variable selon le type d'évènement à traiter.

Cette structure, dont les membres sont en relation permanente, est chargée de gérer toutes les étapes de traitement de l'évènement depuis sa transmission jusqu'à sa conclusion (analyse, diagnostic, mesures de protection immédiates, identification et mise en œuvre des solutions, tests et validation, …) sauf à alerter le responsable de plan de continuité d'activité dans une situation de rupture de service (le lien entre PCA et gestion d'incidents est évoqué en fin d'article).

Elle procède tout d'abord à une étude approfondie des causes et des conséquences du problème signalé. À partir de cet examen, comme au fil de la résolution de l'incident, il peut être fait appel, à tout moment, à d'autres membres de la Cellule de traitement ou à des experts métiers en tant que de besoin, internes et (ou) externes, selon les exigences du dossier et les priorités établies avec les Autorités de l'entreprise.

Il est sûr que l'efficacité de l'équipe dépendra des compétences individuelles de ses membres, mais aussi de leur performance collective, c'est-à-dire de la qualité de leur travail en collaboration.

PARALLELEMENT AU DIAGNOSTIC ET A LA MISE AU POINT DE LA SOLUTION …

A partir des premiers éléments collectés, sur site, par téléphone, … sauvegardes, modification de contexte, installation de correctifs … les intervenants doivent déterminer et mettre en œuvre le plus vite possible les premières mesures destinées si ce n'est à mettre fin, au moins à circonscrire les problèmes et leur propagation et limiter leurs conséquences.

Également, si c'est nécessaire, le coordonnateur prévoit et organise les moyens d'aide compensatoire aux utilisateurs pénalisés par l'incident.

Et puis, s'il s'agit d'un incident technique, il convient de tester et de valider les éléments de la solution avant de les mettre en place en milieu de production.

Alerte, évaluation, diagnostic, traitement, mais aussi … communication

La Direction doit conserver la maîtrise de l'information dans toutes les situations, particulièrement en cas de crise ou, tout au moins de dysfonctionnement, afin d'éviter la propagation de rumeurs et d'interprétations non contrôlés en interne et à l'extérieur.

Il faut, jusqu'à la conclusion de l'incident, informer rapidement et régulièrement les parties intéressées, les personnels, mais aussi les partenaires et les clients.

Par conséquent, un volet communication est à inscrire formellement au dispositif.

ET PUIS QUELQUES RECOMMANDATIONS …

L'INTEGRITE DES DEMARCHES DEPEND AUSSI DU RESPECT DE QUELQUES RECOMMANDATIONS ELEMENTAIRES A PRENDRE EN COMPTE DANS LA PROCEDURE :

- Les initiatives individuelles de correction ou de démonstration d'une faille ou d'une vulnérabilité sont expressément interdites
- Les interventions sont accomplies par du personnel compétent et habilité
- Les informations sont accessibles sous contrôle d'accès aux seules personnes autorisées selon leur rôle et responsabilités
- L'incident, la faille, la vulnérabilité à l'origine du signalement fait l'objet d'une description détaillée confidentielle distincte de la fiche incident
- Le circuit d'échanges ne contient pas d'autres données à caractère personnel que les coordonnées professionnelles indispensables des personnes associées à la démarche, le déclarant et les intervenants.
- L'auteur du signalement est tenu informé de la suite donnée à sa démarche
- Les éléments de preuves sont conservés dans des conditions définies par des compétences juridiques pour pouvoir servir, le cas échéant dans une recherche en responsabilité
- L'incident, par sa nature, sa portée, sa solution, peut exiger des mesures d'accompagnement pour le retour à un service normal. Cette étape doit être traitée dans la procédure …

AVANT DE CLORE LE DOSSIER, UN BILAN POUR RETENIR ET POUVOIR UTILISER TOUS LES ENSEIGNEMENTS D'UN INCIDENT

C'est l'un des intérêts essentiels de la gestion des évènements de sécurité, le bilan à l'issue de chaque affaire doit permettre d'améliorer le niveau de sécurité de l'entreprise notamment par la mise en place d'actions et de mesures correctives et préventives pour que l'incident ne se reproduise pas.

Et si, malgré tout, ultérieurement, des problèmes identiques ou similaires se produisent, les connaissances, l'expérience acquises par cette gestion concrète des risques pourra être réutilisées.

Pour cela, le dispositif en place doit prévoir, à la fermeture du dossier, l'enregistrement de ses caractéristiques dans une base de connaissances.

GESTION DES EVENEMENTS DE SECURITE ET PLAN DE CONTINUITE D'ACTIVITE

Il n'est pas toujours possible de déterminer si un incident va se prolonger jusqu'à empêcher la poursuite de l'activité.

Faut-il pour autant informer systématiquement le Responsable de Plan de Continuité d'Activité de tout évènement de sécurité porteur de conséquences potentielles pour le système d'information ?

Systématiquement, non, car les incidents / évènements sont de nature et de portée très différentes. Par contre, dans les situations où des incertitudes importantes pèsent sur les risques de propagation, les conséquences et la durée de l'incident il est recommandé de l'informer. C'est lui seul qui est habilité à déterminer s'il faut, et quand il faut, réunir le Comité de crise inscrit au P.CA.

Évidemment, toute situation de mise en cause de la continuité de service doit lui être transférée sans délai pour gestion.

Ainsi, l'estimation de l'impact et de la durée d'un incident peut évoluer au cours de son traitement. Dans un sens positif, mais aussi dans un sens négatif. L'incident est plus grave que les premiers éléments le laissaient penser. Il peut hypothéquer la poursuite d'activités essentielles pour l'entreprise.

C'est pourquoi, la procédure doit-elle prévoir des mécanismes d'escalade vers le plan de continuité d'activité à partir, autant que possible, de critères clairement définis qui s'appuient sur les ressources critiques listées au PCA, les délais d'interruption maximale et les perte de données admissibles, sans attendre de les avoir atteints, bien évidemment, pour partager le dossier avec l'autorité en charge du plan de continuité d'activité (ex. telle application ne doit pas être indisponible plus de ***).

Il existe un lien absolu entre les deux processus pour garantir la disponibilité et la continuité de service. C'est dans le titre de notre article. La gestion d'un incident de sécurité ne doit pas être confondue avec le plan de continuité, mais,… elle ne dispense pas d'en avoir un !

EN CONCLUSION

Un système de détection et de correction de problème de sécurité n'est pas figé. Il doit évoluer à partir des observations faites au fil des gestions afin d'améliorer son efficience.

Communication, sensibilisation, initiations aux risques, travail en collaboration, engagement … l'article nous donne l'opportunité de rappeler un principe de pilotage et d'organisation des gestions de la Sécurité de l'Information, les solutions ne sont pas que techniques, loin de là.

L'efficacité des dispositifs en place repose avant tout sur la vigilance, la réactivité et le respect par chacun des mesures et des moyens prévus pour protéger le patrimoine informationnel de l'entreprise et par la capacité de réviser le système de protection très vite lors de la découverte de nouvelles failles ou vulnérabilités.

Et puis, important, la gestion des incidents n'est pas une démarche de sécurité isolée et circonstancielle.

Elle prend tout son sens et toute son efficacité dans le cadre d'un système global de management de la sécurité de l'information tel que défini à la norme Iso 27001.

Enfin, pour terminer, je le confirme, cet article n'a pas d'autre prétention que de faire partager à ses lecteurs une expérience avec ses limites.

Il a pour objet de vous inciter, si ce n'est pas encore fait, à mettre en place un dispositif de gestion des incidents, mais, à la condition de lire auparavant la norme ISO 27035 et quelques ouvrages d'experts dans le domaine.

Il souhaite également susciter vos commentaires pour compléter et fiabiliser l'information qu'il vous propose.

Pour cela, vous avez une adresse électronique à votre disposition
✉ guillet.lionel@gmail.com

À L'ATTENTION DE CEUX QUI DOUTERAIENT ENCORE DE LA NECESSITE DE METTRE EN PLACE LES MOYENS DE GERER LA SECURITE ET SES INCIDENTS

LA GENERALISATION DE L'OBLIGATION DE NOTIFIER LES INCIDENTS DE SECURITE A DES AUTORITES NATIONALES HABILITEES EST EN MARCHE

L'Union européenne a mis en place fin août 2013 l'obligation de notifier formellement toute violation de données à caractère personnel auprès d'une autorité de contrôle pour les opérateurs et les fournisseurs de service de communication.

C'est une première étape. Une règle de portée générale est en préparation et ce ne sont pas que les données à caractère personnel qui sont concernées.

Parallèlement, en France la Loi de Programmation Militaire de décembre 2013 assujettit également les "opérateurs d'importance vitale" à diverses obligations, notamment également celle de notifier toute faille de sécurité dans leur système d'information.

Alors, il faut être prêt. Et comment l'être de meilleure façon qu'en mettant en place sans attendre un système organisé de remontée, de traitement et de mémorisation des incidents de sécurité dans le cadre d'un management maîtrisé des risques et des actions de protection.

C'est pourquoi, nous voyons avantage à développer ce sujet dans un article séparé « conformité réglementaire, levier du développement de la sécurité de l'information ».

GESTION DES EVENEMENTS ET DES INCIDENTS DE SECURITE

EN RESUME

Politique / Processus / Procédure de gestion des évènements & des incidents de sécurité
Enjeux, objectifs, organisation, périmètre, définition précise des évènements pris en compte, des rôles et des responsabilités, détermination des circuits, identification des intervenants, coordination et suivi, traitement, …
Contexte en place, l'action est portée par la communication qui convient.

Étape 1
Détection des évènements

Vigilance et réactivité de l'ensemble des utilisateurs du système d'information de l'entreprise.
Préalable … information, sensibilisation, Initiation aux risques

Étape 2
Alerte
Signalement

Alerte dans les délais les plus brefs, téléphone, messagerie … mais, surtout, utilisation d'un formulaire, support de base du dispositif, complété au fil du traitement du problème.
Envoi à un interlocuteur unique identifié.

Étape 3
Management
Identification
Évaluation
Mise en œuvre du dispositif

Direction, service, manager des risques … examen de l'alerte par un responsable unique, point d'entrée du système.
Classification de l'évènement (juridique, ress. humaines, informatiques, matériel …)
Évaluation de portée, d'impact et de durée. Validation ou … exclusion ou … escalade vers le plan de continuité d'activité
Constitution de la cellule de traitement.
Coordination et suivi de traitement de l'incident.

Étape 4
Traitement collégial
Analyse
Diagnostic
Solution

Analyse, diagnostic et mise au point de la solution par une cellule de spécialistes dont la composition dépend de la nature de l'évènement.
La liste des experts est préétablie. Ils peuvent se faire aider à tout moment par des compétences internes ou externes.
En relation permanente avec le point d'entrée chargé du suivi de traitement.

Étape 5
Etape intermédiaire
Mesures urgentes

Première analyse
Mesures conservatoires et de limitation des risques d'extension (sauvegardes, déconnexion, correctifs …) au plus tôt dans la procédure.
Mesures de soutien opérationnelles temporaires (aide R.H., postes de travail …)

Étape 6
Tests et validation de la solution

Si nécessaire, la solution corrective mise au point est testée et validée avant sa mise en place en réel.

Étape 7
Mise en place de la solution

Mise en œuvre de la solution en milieu utilisateur et suivi pour tenir compte des risques de récurrence, de propagation masquée ou de mise en évidence de nouveaux dysfonctionnements après correction.
Accompagnement au retour en service normal si la situation l'exige.

Étape 8
Bilan
Retour d'expérience

Mise en place de mesures et de solution préventives / correctives
Enrichissement d'une base des incidents pour réutilisation des informations pour un évènement similaire
Evaluation de la performance du dispositif

Ne pas oublier

- Servir la communication fonctionnelle, opérationnelle et la communication générale interne et externe
- Garantir la maîtrise des interventions
- Préserver la confidentialité des données sensibles
- Assurer la conformité de conservation des éléments de preuve
- Informer le déclarant de la suite donnée à son alerte ….

LES COMMENTAIRES APPORTÉS PAR LES LECTEURS DE L'ARTICLE

Cette annexe propose un complément d'informations à partir des commentaires reçus pour cet article.

C'est un apport précieux à l'amélioration de son contenu. Nous remercions vivement leurs auteurs

POURQUOI LA DESACTIVATION D'UN ANTI-VIRUS NE RELEVERAIT-ELLE PAS DE LA GESTION DES INCIDENTS ?

La désactivation de l'anti-virus est un incident, bien sûr.

Sur un, sur quelques postes de travail, c'est un incident informatique courant. Il est signalé au service informatique pour dépannage. Il relève des interventions de maintenance ordinaire (ordinaire et ô combien importante (!)).

Par contre, des désactivations répétées sans identification de la cause, voire une désactivation générale, ou tout au moins sur de nombreuses stations, de l'anti-virus, ces situations demandent à être administrées comme des évènements de sécurité de nature à mettre en danger l'intégrité et la disponibilité du système d'information de l'entreprise, des évènements qui justifient un suivi particulier.

Tout est affaire d'impact, potentiel ou réel.

Le modèle de processus proposé intéresse, en effet, les situations de nature à remettre en cause le système d'information de l'entreprise, son intégrité, sa disponibilité, sa confidentialité et sa conformité.

Ce n'est pas le cas des incidents informatiques courants, du dysfonctionnement ponctuel de l'anti-virus, de la panne d'un disque dur ou même une panne de serveur limitée …

COMMENT FAIRE LA DISTINCTION ENTRE LA SITUATION QUI ENTRE DANS LE DISPOSITIF ET CELLE QUI N'Y ENTRE PAS ?

La distinction n'est pas toujours évidente, mais elle est nécessaire car le processus est exposé à un risque "mortel", l'encombrement et la saturation par la multiplication des alertes injustifiées dont il faut absolument se protéger tout en gardant au dispositif son sens et son efficacité. D'où l'importance de cette distinction à faire entre incident courant et évènement de portée supérieure.

Pour cela, il convient de porter la plus grande attention à l'élaboration du tableau de référence des menaces, avec indication de leur origine, de(s) critère(s) de sécurité affecté(s) et de scénarios illustratifs, comme le propose, par exemple, la méthode EBIOS.

Un tableau à mettre à jour en tant que de besoin.

Un tableau à compléter par une proposition de contact téléphonique en cas de doute sur le caractère d'un incident.

C'est bien un tel contexte qui doit permettre de progresser collectivement en connaissance sur la perception et la protection contre les risques, l'un des avantages essentiels attendus du dispositif.

LE REFERENTIEL DE BONNES PRATIQUES ITIL PREVOIT NOTAMMENT UN SERVICE, UNE ORGANISATION DE LA GESTION DES INCIDENTS. NE PEUT-IL PAS S'APPLIQUER ?

La mise en place d'un processus de gestion des évènements / incidents de Sécurité de l'Information, au sens des normes Iso de la famille des 27 000, ne remet pas en cause une approche de type ITIL de la part des services informatiques.

En effet, le référentiel ITIL, repris dans la norme Iso 20 000[4], publie des règles de bonnes pratiques afin d'améliorer la qualité et l'efficience du département informatique dans le cadre d'une relation client / fournisseur avec les services de l'entreprise. Le traitement des incidents et des problèmes en font partie, mais uniquement en matière informatique.

Alors que la norme Iso 27 001, et sa suite, s'attache, elle, aux conditions et modalités de gestion de la Sécurité de l'Information dans tous les domaines où elle doit s'exprimer, l'informatique, certes, mais aussi, les sécurités physiques, les ressources humaines, la conformité juridique, l'organisation, etc.

Par conséquent, un incident informatique peut parfaitement entrer dans la boucle de traitement de type ITIL / Iso 20 000 mise en place par votre service informatique, sans que le dispositif de gestion des évènements de Sécurité de l'Information dans le cadre normatif 27 001 ait à en connaître, sauf si … la portée de l'incident réelle ou suspectée le justifie.

Pour reprendre notre exemple, une désactivation d'ampleur de l'anti-virus relève bien, par sa portée, d'une approche de type 27 001. L'incident entre dans le dispositif, alors que la désactivation ponctuelle de l'anti-virus sur un poste n'y entre pas, mais tous les deux peuvent parfaitement souscrire aux protocoles ITIL.

Sans tomber dans la bureaucratie et le formalisme, car, le temps est compté, nous nous inscrivons bien dans la volonté partagée de travailler ensemble afin de servir une cause commune, assurer à l'entreprise la protection et l'intégrité de son patrimoine informationnel et des moyens indispensables à sa valorisation au service des activités.

C'est ainsi particulièrement vrai, pour répondre à un autre commentaire, sur l'urgence à reconnaître aux dispositions conservatoires à prendre afin de limiter les conséquences négatives de l'incident.

LE MOYEN D'ALERTE LE PLUS SOUVENT UTILISE EST LE HELPDESK. POURQUOI N'EN PARLEZ-VOUS PAS ?

Le helpdesk est réservé à l'assistance et aux maintenances informatiques. Il entre dans un système de type ITIL. Il n'est pas remis en cause, bien au contraire.

En effet, placé en situation de recevoir et de traiter les informations de son domaine, il est partenaire majeur du dispositif, dans l'analyse et le traitement mais aussi dans l'alerte.

[4]Normes Iso 20 000 et 27 001 - Les deux normes sont compatibles. Elles sont même complémentaires. N'est-ce pas d'ailleurs la norme Iso 27013, toute nouvelle, qui considère tous les avantages qu'une organisation peut attendre d'une approche combinée des mesures de qualité applicables aux Services Informatiques et des mesures applicable en matière de Sécurité de l'Information ?

Par exemple, le service informatique reçoit séparément de nombreux appels pour signaler la désactivation de notre anti-virus de tout à l'heure (toujours lui !). Il lui appartient d'alerter le point d'entrée du dispositif de gestion des incidents de Sécurité de l'Information.

C'est toujours affaire de portée et d'impact réels ou potentiels.

LE DECLARANT EST-IL TOUJOURS EN MESURE DE QUALIFIER UN INCIDENT ?

Non, certainement pas. Soit, parce que l'évènement n'entre pas dans la liste des risques prévus (qu'il faudra mettre à jour !) soit, il subsiste des incertitudes d'interprétation du référentiel publié.

Cette situation ne doit pas remettre en cause le signalement à effectuer. Un échange téléphonique, avant, pendant ou après l'envoi du signalement, doit permettre de lever toute ambiguïté.

LE CLUSIF A FAIT UN TRAVAIL REMARQUABLE DANS LE DOMAINE

C'est exact. Il a publié un document de référence sur le sujet, un document dont je vous invite à prendre connaissance si vous ne l'avez pas encore fait.

Il s'agit d'un guide qui ne peut qu'alimenter utilement notre perception et notre réflexion sur les mécanismes fonctionnels et opérationnels à mettre en œuvre.

Il est complété d'une seconde partie qui propose, sous forme de fiches, des informations pratiques sur la marche à suivre dans certains incidents informatiques précis.

Il faut savoir aussi que le Club de la Sécurité de l'Information Français reprend son travail sur le sujet en 2013 avec la publication de la norme ISO 27 035 et, notamment, ses liens avec d'autres normes comme … la norme ISO 20 000 (!)

À suivre donc, avec beaucoup d'intérêt.

INFORMER LE RESPONSABLE DU PLAN DE CONTINUITE D'ACTIVITE SANS DELAI RISQUE DE SURCHARGER L'INTERESSE. IL CONVIENT DE TROUVER LE BON ENDROIT OU PLACER LE CURSEUR.

"IL EST RECOMMANDE D'INFORMER LE RPCA". IL DOIT Y AVOIR DES CRITERES CLAIREMENT DEFINIS POUR LA PLUPART DES RISQUES.

La rubrique consacrée au sujet "Gestion des évènements et plan de continuité d'activité" a été modifiée pour tenir compte de ces observations.

La perception des risques et des moyens de s'en préserver est un des avantages majeurs attendus de ce type de dispositif. Pourquoi ne pas le faire valoir dès la présentation du sujet ?

En effet, pourquoi pas. Alors …

DANS LE SCHEMA, IL FAUT INDIQUER QU'UN INCIDENT PEUT ETRE ITERATIF OU QU'IL PEUT EN CACHER UN AUTRE

L'étape 7 a été mise à jour en ces termes " Mise en œuvre de la solution en milieu utilisateur et suivi pour tenir compte des risques de récurrence, de propagation masquée ou de mise en évidence de nouveaux dysfonctionnements après correction".

ANNEXE 2

SECURITE DE L'INFORMATION

[UN FORMULAIRE BASIQUE POUR EXEMPLE
LA NORME 27035 ANNEXE UN SUPPORT PLUS COMPLET]

RAPPORT D'INCIDENT
REMONTEE D'INFORMATION
SUIVI DU TRAITEMENT

COORDONNEES DU POINT D'ENTREE _____

---------- Partie complétée par le déclarant ----------

DATE DU SIGNALEMENT : _____

IDENTITE DU DECLARANT

NOM	**SERVICE OU SOCIETE**
TELEPHONE	**EMAIL**

IDENTIFICATION DE L'INCIDENT DE SECURITE
Préserver l'anonymat des informations

TYPE INCIDENTS DE SECURITE [TABLEAU DES RISQUES EN ANNEXE]	**ORIGINE [*]**			**CRITERES DE SECURITE AFFECTES**		
	A	**E**	**M**	**D**	**I**	**C**
Ex. Panne matériel	A			X	X	

Pour vous aider à compléter le tableau

(*)**ORIGINE** : **A** – Accident/défaillance technique / **E** – Erreur/Maladresse
M – Malveillance/Acte délibéré

Les **CRITERES DE SECURITE AFFECTES** s'apprécient à partir des questions suivantes :

LA DISPONIBILITE [D] L'incident a-t-il privé l'utilisateur des moyens informatiques nécessaires à son activité ?

L'INTEGRITE [I] Les données et les traitements ont-ils subi, ou auraient-ils pu subir, une altération lors de l'incident ?

LA CONFIDENTIALITE [C] L'incident a-t-il provoqué une faille dans la protection des accès aux informations et aux traitements considérés ?

Il est à noter qu'un dysfonctionnement peut mettre en cause simultanément plusieurs critères de sécurité.

C'est l'exemple pris dans la grille ci-dessus. La panne d'un matériel causée par une défaillance technique (ou une erreur d'utilisation) peut avoir des conséquences en termes de disponibilité d'équipement, mais aussi en termes d'intégrité par altération ou perte d'information.

---------- Partie complétée par le point d'entrée ----------

RESOLUTION DE L'INCIDENT DE SECURITE

DATE DE DEBUT DU TRAITEMENT:
DATE DE FIN DU TRAITEMENT :
NOM(S) DE(S) MEMBRES DE L'EQUIPE D'INTERVENTION
NOM(S) DE(S) SUPPORT(S) ASSOCIE(S) AU TRAITEMENT
NOM(S) DE(S) INTERVENANT(S) EXTERIEUR(S)
IDENTIFICATION DU TYPE D'AUTEUR DE L'INCIDENT : Individu – Accident – Groupe organisée – Pas d'auteur
DESCRIPTION DE L'AUTEUR :
MESURES D'URGENCE
MESURES COMPENSATOIRES DE SOUTIEN A L'ACTIVITE
MESURES PRISES POUR RESOUDRE L'INCIDENT
MESURES DE SUIVI PLANIFIEES - ACTIONS EN COURS (Le cas échéant)
MESURES DE RETOUR EN SERVICE NORMAL
MESURES PREVENTIVES PRECONISEES
DATE DU RETOUR D'INFORMATION A L'AUTEUR DU SIGNALEMENT :

REMONTEE D'INFORMATION

AUTORITES INFORMEES

BILAN ET CONCLUSIONS

DATE ET SIGNATURE

QUELQUES PRECISIONS –

- Cette fiche incident est complétée en tant que de besoin par un descriptif détaillé de l'incident / évènement. C'est un support confidentiel. Il contient des informations sensibles, des informations sur les vulnérabilités du système d'information de l'entreprise.

- Vous avez noté en Page 1 du modèle, un tableau des risques pour aider à l'identification de l'incident de sécurité.

Ce tableau comprend :

- Une brève description de chaque scénario de risques génériques
- Les critères de sécurité affectés (disponibilité, intégrité, confidentialité, voire authenticité, si vous le souhaitez)
- L'indication de l'origine (l'accident, l'erreur, la malveillance).

Les référentiels de la méthode EBIOS sont à votre disposition pour établir votre référentiel. Ce ne sont pas les seuls.