Ligne directrice sécurité de l'information et vie privée

Gestion des incidents

(BLD INCID)

TABLE DES MATIERES

1. Introduction

Le présent document fait intégralement partie de la méthodologie de sécurité de l'information et la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution de sécurité sociale. Le maintien, le suivi et la révision du présent document relèvent de la responsabilité du service sécurité de l'information de l'institution de sécurité sociale.

La gestion des incidents ainsi que la politique de sécurité de l'information, la gestion des risques et la gestion de la continuité constituent les principaux domaines d'attention des normes minimales. La gestion des incidents est primordiale puisqu'il n'est pas possible de garantir 100% de sécurité de l'information et de protection de la vie privée et qu'il est impossible de prévenir des incidents. La question n'est pas de savoir si quelque chose va se passer mais bien à quel moment. Il y a lieu de réfléchir à l'avance aux principaux incidents qui pourraient se produire et donc aussi mettre au point au préalable une procédure de réaction et d'escalation appropriées.

La gestion d'incident de l'organisation indique la façon dont l'organisation souhaite traiter tous les incidents et «incidents proches» dans le domaine de la sécurité de l'information et de la vie privée. L'organisation approuve l'importance d'un traitement adéquat des incidents et la réponse à la minimisation de l'impact sur le fonctionnement de l'organisation. Les incidents doivent être traités de manière structurelle et des procédures doivent être établies pour permettre une réponse efficace et ordonnée aux incidents. L'organisation va apprendre des incidents et donc les incidents doivent être évalués.

La gestion des incidents sur le plan de la sécurité de l'information et de la vie privée comprend la surveillance et la détection d'incidents de sécurité (security events) sur un ordinateur ou un réseau d'ordinateurs (data breaches), mais aussi la constatation d'activités suspectes par les collaborateurs de l'institution et l'apport des réponses exactes à ces événements.

La gestion des incidents est le processus par lequel les systèmes d'information et les informations y enregistrées sont gérés et protégés. Les institutions doivent être conscientes de leurs responsabilités dans la protection de ces informations pour les citoyens et autres institutions. Fait aussi partie de cette responsabilité, la possession d'un plan des étapes à suivre pour savoir "que faire si quelque chose échoue". La gestion des incidents est un ensemble d'activités qui définit et met en œuvre un processus qu'une institution peut utiliser pour son propre bien-être et la sécurité du public.

2. Gestion des incidents

Toute organisation souscrit les directives suivantes de sécurité de l'information et protection de la vie privée pour toutes les informations et systèmes d'information qui relèvent de la responsabilité de l'organisation.

1. Il y a lieu de fixer des responsabilités et d'établir des procédures qui doivent faire l'objet d'une communication claire et précise au sein de l'organisation. Ces procédures doivent être connues auprès de tous les collaborateurs.
2. Chaque collaborateur (que ce soit à contrat indéterminé ou temporaire, interne ou externe) doivent signaler des accès non authorisés, l'utilisation, le changement, la publication, la perte ou la destruction des informations et des systèmes de l'information.
3. Les évènements et les faiblesses sur la sécurité de l'information ou vie privée qui sont liées avec l'information et les systèmes TIC doivent être signalés pour que l'organisation puisse prendre des mesures correctives à temps et adéquates.
4. Les incidents sur la sécurité de l'information et vie privée doivent toujours être communiqués dans les meilleurs délais vers le helpdesk, le délégué à la protection des données (DPO) ainsi qu'au conseiller en sécurité de l'information (CISO).

5. Les incidents sur la sécurité de l'information et vie privée exigent de collecter et garder toutes évidences pouvant servir de preuve dans le cadre d'une investigation criminalistique.
6. Chaque incident sur la sécurité de l'information et vie privée doit être formellement évalué afin d'améliorer les procédures et mesures de contrôle. Les leçons de l'incident doivent être communiquées à la direction de l'organisation afin de valider et approuver des actions nécessaires.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description du changement	Date approbation	Date entrée en vigueur
2007		V2007	Première version	10/10/2007	10/10/2007
2017		V2017	Intégration UE GDPR	07/03/2017	07/03/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", september 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", september 2013, 80 p.
- ISO, "ISO/IEC 27035:2016 part 1 Information security incident management -- Part 1: Principles of incident management", november 2016, 21 p.
- ISO, "ISO/IEC 27035:2016 part 2 Information security incident management -- Part 2: Guidelines to plan and prepare for incident response", november 2016, 57 p.
- ISACA, "COBIT 5 for Information Security", Mei 2012, 220 p.
- CCB, "Gids voor incidentbeheer", februari 2016, 38 p.
- NIST, "Computer Security Incident Handling Guide", Augustus 2012, 70 p.

- Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:
- https://www.iso.org/isoiec-27001-information-security.html
- https://www.iso.org/standard/54534.html
- https://www.iso.org/standard/60803.html
- https://www.iso.org/standard/62071.html
- http://www.isaca.org/cobit
- https://wiki.en.it-processmaps.com/index.php/Incident_Management
- http://www.ccb.belgium.be/sites/default/files/documents/CSIMG_2016_FR.pdf
- https://www.cybersimpel.be/fr

Annexe C: Principes relatifs à la gestion des incidents

Responsabilité et mise au point de procédures

Objectif: Etablir des responsabilités et des procédures de manière proactive afin de pouvoir offrir une réponse rapide, effective et ordonnée aux incidents liés à la sécurité de l'information et à la vie privée.

Directives

Il y a lieu de fixer des responsabilités et d'établir des procédures qui doivent faire l'objet d'une communication claire et précise au sein de l'institution. Les thèmes suivants doivent être traités:

a) Comment gérer les incidents (identifier, endiguer, éliminer et rétablir et activités postérieures à l'incident)

b) Surveiller, détecter, analyser et rapporter des événements et incidents

c) Enregistrer les incidents

d) Comment traiter les preuves criminalistiques

e) Evaluer les événements et prendre des décisions y relatives (lesquelles)

f) Comment évaluer les failles au niveau de la sécurité de l'information et/ou de la vie privée

g) Faire remonter les incidents

h) Comment rétablir une situation normale suite à des incidents

i) Qui communique quoi et comment aux collaborateurs de l'institution et aux autres personnes concernées.

Le rapportage d'incidents doit avoir lieu de manière standard, afin de garantir un déroulement efficace et efficient.

En ce qui concerne les communications non automatisées d'événements, il y a lieu de répondre aux questions suivantes:

a) Quel était l'événement

b) Qui a constaté les faits

c) Quand l'événement a-t-il eu lieu

d) Quand les faits ont-ils été constatés

e) Qu'est-ce qui a causé l'événement

f) Comment les faits ont-ils été constatés

g) Qu'est-ce qui a influencé l'événement

h) L'impact (potentiel) de l'événement sur les activités de l'institution.

En ce qui concerne les communications automatisées, voir le document relatif à la policy "logging".

Rapporter des failles

Objectif: les travailleurs et tiers utilisant les services et systèmes d'information de l'institution doivent rapporter directement toute faille observée ou supposée dans les services ou systèmes d'information.

Directives

- Lorsque les collaborateurs internes ou externes de l'institution présument ou détectent des failles, ils doivent les signaler dans les meilleurs délais.

- Il faut ajouter une référence vers le TLP code (voir document sur DATA Classification).
- Les utilisateurs doivent savoir qu'ils ne peuvent, en aucune hypothèse, essayer d'exploiter des failles dans la sécurité de l'information ou dans la protection de la vie privée.

Identifier et rapporter des événements

Objectif: identifier et rapporter les événements dans les meilleurs délais via les canaux appropriés

Directives

Un incident-a-t-il effectivement eu lieu? Y-a-t-il une infraction à la sécurité de l'information ou à la vie privée? Cette activité concerne normalement uniquement le gestionnaire système et l'utilisateur final, mais peut être consécutive à la détection proactive d'incidents par la sécurité ICT ou la gestion système, à la remontée d'éléments lors du contrôle des loggings. S'il est constaté qu'il s'agit effectivement d'un incident de sécurité, il y a lieu d'avertir les parties concernées.

- Il y a lieu d'informer l'ensemble des collaborateurs sur leurs responsabilités de signaler les événements présumés en rapport avec la sécurité de l'information et la vie privée, à un point de contact central, dans les meilleurs délais. Par ailleurs, ceux-ci doivent être au courant de la procédure à suivre pour signaler ces types d'événements.
- Pour les situations suivantes (liste non exhaustive), il y a lieu de déterminer si elles doivent ou non faire l'objet d'une communication:
    - Contrôle ineffectif de la sécurité
    - Infraction à l'intégrité, à la confidentialité ou à la disponibilité de données
    - Erreurs humaines relatives à la sécurité de l'information
    - Non-respect de procédures ou de directives relatives à la sécurité de l'information
    - Infraction à la protection physique
    - Infraction à la vie privée
    - Changements incontrôlés dans les systèmes
    - Dysfonctionnement des logiciels ou du matériel
    - Infractions à la politique d'accès.
- Il faut donner un feedback concernant les actions entreprises à l'instance compétente (ou aux instances compétentes). En fonction des suites de l'action entreprise, la personne qui a signalé l'événement peut également être informée par les instances compétentes.

Evaluer des événements / prendre une décision relative

Objectif: Evaluer des événements et décider s'il y a lieu de les qualifier d'incidents

Directives

Le chef de la section où un incident se produit désigne un "chef réaction incident" et constitue une équipe incident propre à l'incident. Le chef informe et demande si nécessaire de l'aide au conseiller en sécurité de l'information (CISO) ou au délégué à la protection des données (DPO). Suite à une fuite de données à caractère personnel, il faut toujours informer le délégué à la protection des données (DPO) et aussi le conseiller en sécurité de l'information (CISO). En cas d'incidents majeurs, le conseiller en sécurité de l'information (CISO) assumera, dans la plupart des cas, la fonction de chef d'équipe. Cette équipe est chargée de limiter les dégâts futurs suite à l'incident. Une évaluation approfondie de la nature et de l'ampleur de l'incident ainsi que des dégâts est réalisée et les preuves sont mises en sécurité. En cas de fuite de données, les informations doivent être transmises à la Commission de la protection de la vie privée dans les 72 heures après la constatation.

- Il y a lieu d'établir des critères pour une classification uniforme des incidents liés à la sécurité de l'information et à la vie privée.
- Le point de contact où les événements doivent être signalés doit appliquer une classification uniforme sur la base de laquelle l'événement doit être considéré comme un événement ou un incident.
- L'évaluation et les décisions en rapport avec les événements peuvent être transmises par le point de contact au conseiller en sécurité de l'information (CISO) ou au délégué à la protection des données (DPO) qui doit confirmer l'évaluation ou la décision ou qui doit à nouveau évaluer.
- Les résultats des évaluations et des décisions doivent être enregistrés avec suffisamment de détails de sorte que ceux-ci puissent servir de référence ou d'éléments de vérification pour les événements/incidents futurs.

Collecte et mise en sécurité des preuves

Objectif: définir des procédures permettant d'identifier, de collecter et de garder intactes les informations relatives aux incidents (qui peuvent servir de preuve dans le cadre d'une investigation criminalistique).

Directives

- Il y a lieu de rédiger des procédures décrivant comment utiliser les preuves, en vue d'actions disciplinaires et/ou légales.
- Ces procédures doivent décrire comment les preuves doivent être identifiées, recueillies et conservées, compte tenu des différents types de média.
- Les procédures d'utilisation des preuves doivent tenir compte:
    - de la chaîne des preuves
    - de la protection des preuves
    - de la protection des collaborateurs de l'institution, des visiteurs ou des citoyens
    - des rôles et responsabilités des collaborateurs, visiteurs ou citoyens concernés
    - de la compétence des collaborateurs de l'institution
    - de la documentation et de l'enregistrement
    - du rapportage
- La certification ou d'autres méthodes doivent être utilisées pour garantir du personnel qualifié ou l'adéquation des outils, de sorte que la valeur des preuves puisse être renforcée.
- Si la collecte de preuves criminalistiques dépasse les limites organisationnelles et/ou juridiques, il y a lieu de vérifier si l'organisation est autorisée à recueillir les informations utiles en tant que preuves criminalistiques.

Réagir aux incidents et les réparer

Objectif: Réagir aux incidents et les réparer conformément aux procédures pertinentes

Directives

Il y a lieu de prendre des mesures afin de bloquer ou supprimer la cause de l'incident, de réduire l'impact en évitant l'exposition des données sensibles, de relancer les processus si ceux-ci avaient été arrêtés suite à l'incident et de réduire les risques liés à cet incident.

- Les incidents doivent être traités via un point de contact central.
- Les preuves doivent être récoltées le plus rapidement possible après l'incident.

- Si nécessaire, il y a lieu de réaliser une analyse criminalistique.
- Si nécessaire, il y a lieu de procéder à une remontée de l'incident.
- Les actions entreprises doivent être enregistrées.
- Les collaborateurs de l'organisation et des tierces parties doivent être informés de l'incident, sur une base 'need-to-know'.
- Il y a lieu de réaliser une analyse postérieure à l'incident afin de déterminer la cause de l'incident.
- Les failles qui ont causé l'incident ou qui y ont contribué, doivent être analysées et résolues.
- Un incident qui a été traité avec succès doit être finalisé et rapporté de manière formelle.
- Toute réaction aux incidents doit donner lieu au rétablissement d'un fonctionnement normal et à la prise des procédures de rétablissement nécessaires.
- Il y a lieu d'utiliser un seul système central de gestion des incidents (outil) qui enregistre l'ensemble des informations relatives aux événements et incidents.
- Outre la date et l'heure de l'incident de sécurité de l'information, les éléments suivants sont aussi documentés:
    - Qu'est-ce qui a été constaté, quelles actions ont été entreprises (aussi utilisation d'outils automatiques) et pourquoi
    - L'emplacement des preuves
    - Si d'application, comment et où les preuves ont-elles été conservées?
    - Si d'application, comment les preuves ont-elles été vérifiées?
    - Un aperçu des preuves.

Tirer des leçons des incidents au moyen d'un rapport et d'une évaluation

Objectif: Utiliser les leçons tirées de l'analyse et de la résolution d'incidents pour réduire la probabilité ou l'impact d'incidents futurs

Directives

Identifiez les leçons de l'incident et discutez-en avec l'équipe, faites un rapport sur l'incident, les mesures prises et le rapport, rapportez si nécessaire au niveau interne et externe, adaptez si nécessaire le plan des étapes à suivre.

- Des processus et des outils doivent être disponibles pour quantifier et surveiller le type, le volume et le coût des incidents.
- Les informations recueillies sur les incidents doivent être utilisées pour identifier les incidents récurrents à impact élevé.
- L'évaluation des incidents doit être utilisée afin de vérifier que les contrôles actuels sont adéquats. Si nécessaire, les contrôles doivent être adaptés.

Signaler les incidents relatifs à la vie privée

Objectif: les incidents relatifs aux données à caractère personnel doivent être signalés dans les 72 heures à la Commission de la vie privée

Directives

En cas d'incident relatif à des données à caractère personnel, le responsable du traitement notifie cet incident à la Commission de la vie privée, dans les meilleurs délais et, si possible, dans les 72 heures après en avoir pris

connaissance, à moins que l'incident relatif aux données à caractère personnel ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes. Si la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle doit s'accompagner d'une motivation du retard.

Le sous-traitant informe le responsable du traitement, dans les meilleurs délais, dès qu'il a pris connaissance d'une infraction relative à des données à caractère personnel:

a) la nature de l'incident lié aux données à caractère personnel, avec si possible l'indication des catégories des intéressés et des registres de données à caractère personnel concernés et, approximativement, le nombre de personnes et de registres de données à caractère personnel concernés;

b) le nom et les données de contact du délégué à la protection des données (DPO) ou un autre point de contact où davantage d'informations peuvent être obtenues;

c) les conséquences probables de l'incident lié aux données à caractère personnel;

d) les mesures que le responsable du traitement a proposées ou a prises afin de résoudre l'incident lié aux données à caractère personnel, parmi lesquelles, le cas échéant, les mesures limitant leurs effets négatifs éventuels.

Dans la mesure où il n'est pas possible de transmettre toutes les informations en même temps, les informations peuvent être transmises, dans les meilleurs délais, en phases. Le responsable du traitement documente les incidents relatifs aux données à caractère personnel, en indiquant les faits concernant l'incident lié aux données à caractère personnel, son impact et les mesures correctrices prises. Cette documentation permet à la Commission de la vie privée de contrôler le respect.

Lorsqu'il est probable qu'une violation de données à caractère personnel entraîne un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique, dans les meilleurs délais, à la personne concernée, l'incident lié aux données à caractère personnel, au moyen d'une description dans un langage clair et simple:

a) la nature de l'incident

b) les instances qui sont en mesure de fournir davantage d'informations sur l'incident

c) les mesures préconisées pour réduire les effets négatifs de l'incident

La communication à la personne concernée n'est pas requise lorsqu'une des conditions suivantes est remplie:

a) le responsable du traitement a pris des mesures de protection techniques et organisationnelles appropriées et a appliqué ces mesures aux données à caractère personnel sur lesquelles porte l'incident lié aux données à caractère personnel, à savoir des mesures qui rendent les données à caractère personnel illisibles pour les personnes non autorisées, comme par exemple le chiffrement;

b) le responsable du traitement a pris des mesures a posteriori afin de veiller à ce que le risque élevé pour les droits et libertés des intéressés ne se reproduise probablement plus;

c) la communication requiert des efforts disproportionnés.

Dans ce cas, cette communication serait remplacée par une communication publique ou une mesure similaire qui informerait aussi les intéressés en toute efficacité.

La Commission de la protection de la vie privée peut, après délibération sur la probabilité qu'un incident lié à des données à caractère personnel entraîne un risque élevé, obliger le responsable du traitement à réaliser une communication.

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	
Sécurité physique et environnementale	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	**Oui**
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

***** FIN DU DOCUMENT *****