Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2018

ÉPREUVE DE PROJET OU ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options choisie par le candidat, au moment de son inscription, parmi celles prévues à l'annexe du décret n°2016-206 du 26 février 2016.

Durée : 4 heures
Coefficient : 5

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION

OPTION : SYSTÈMES D'INFORMATION ET DE COMMUNICATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 61 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas …

Vous êtes ingénieur territorial au sein de la Direction des Systèmes d'Information et des Services Numériques (DSISN) de la métropole d'INGECO (500 000 habitants).

Une collectivité voisine vient d'être victime d'une cyber-attaque ayant entraîné plusieurs dysfonctionnements majeurs dans le fonctionnement des services. L'incident a été repris dans la presse locale.
Le Président d'INGECO souhaite disposer d'informations relatives à la cybersécurité.

Votre directeur fait appel à vous pour obtenir ces différents éléments.

À l'aide de l'annexe, vous répondrez aux questions suivantes :

Question 1 (5 points)

Dans une note, vous présenterez les enjeux et les objectifs de la cybersécurité et vous analyserez les risques et les principales difficultés dans le contexte de la collectivité.

Question 2 (3 points)

La collectivité souhaite désigner un Délégué à la Protection des Données (DPD) et un Responsable de la Sécurité des Systèmes d'Information (RSSI).
a) Vous rédigerez la fiche de poste du DPD et indiquerez les modalités de sollicitation dudit agent.
b) Vous préciserez les conditions et les modalités d'une mutualisation de ces deux fonctions avec l'ensemble des communes membres.
c) Vous indiquerez les modalités de collaboration éventuelles entre le DPD et le RSSI.

Question 3 (6 points)

Vous exposerez les bonnes pratiques d'usage en matière de sécurisation du réseau informatique.

Question 4 (6 points)

En tenant compte de l'annexe A, vous rédigerez une note à l'attention de votre directeur pour proposer une démarche globale d'amélioration de la cybersécurité de la métropole d'INGECO, en intégrant le rôle des utilisateurs dans votre réflexion.

Liste des documents :

Document 1 : « Le "RGS" ou la sécurité informatique des autorités administratives pour les pas trop nuls » – *Sabine BLANC* – *lagazettedescommunes.com* – mis à jour le 3 octobre 2014 – 2 pages

Document 2 : « Règlement européen sur la protection des données : ce qui change pour les professionnels » – *cnil.fr* – 15 juin 2016 – 7 pages

Document 3 : « Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance » – *Pierre Alexandre CONTE* – *lagazettedescommunes.com* – 23 février 2017 – 4 pages

Document 4 : « ISO/CEI 27001 » – *wikipedia.org* – mis à jour le 21 août 2017 – 5 pages

Document 5 : Cours « Méthodologie de la Sécurité » – *Pierre-François BONNEFOI* – *Faculté des Sciences et Techniques de Limoges* – *p-fb.net* – Version du 10 avril 2017 – 14 pages

Document 6 : « Sécurité informatique : les collectivités territoriales, des cibles qui s'ignorent » – *Pierre-Alexandre CONTE* – *lagazettedescommunes.com* – 18 mars 2016 – 2 pages

Document 7 : « Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures » (extraits) – *Agence nationale de la sécurité des systèmes d'information (ANSSI)* – *Version 2* – Septembre 2017 – 17 pages

Document 8 : « Devenir délégué à la protection des données » – *cnil.fr* – 23 mai 2017 – 6 pages

Liste des annexes :

Annexe A : « Présentation du Système d'Information (SI) d'INGECO » – *DSISN d'INGECO* – 2018 – 1 page – l'annexe n'est pas à rendre avec la copie

Documents reproduits avec l'autorisation du C.F.C.

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

Sécurité informatique

Le “RGS” ou la sécurité informatique des autorités administratives pour les pas trop nuls

Publié le 02/10/2014 • mis à jour le 03/10/2014 • par Sabine Blanc • dans : France • lagazettedescommunes.com

La version 2 du référentiel général de sécurité (RGS) a été publiée par l’Agence nationale de la sécurité des systèmes d'information (Anssi) fin juin. Cette évolution se veut plus accessible que la mouture initiale, jugée trop complexe. Mais l'Anssi a encore du chemin à parcourir vers les collectivités territoriales, si l'on en juge le programme de ses assises qui se tiennent cette semaine.

Utile mais trop complexe : tel était, en bref, le jugement porté sur la première version du référentiel général de sécurité (RGS) publié en 2010 par l’Agence nationale de la sécurité des systèmes d’information (Anssi). La seconde mouture, en application depuis le 1er juillet dernier, devrait répondre à cette critique.

Créé par l’article 9 de l’ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, le RGS est un guide pour accompagner les administrations dans leur marche vers l’administration électronique. Les collectivités territoriales doivent s’y conformer depuis mai 2013 en ce qui concerne les certificats électroniques (arrêté du 6 mai 2010). Il était composé d’un corps d’une trentaine de pages et d’annexes purement techniques.

Avec 25 pages contre 33, la V2 du corps du RGS est effectivement bien moins rebutante. Une cure d’amaigrissement, malgré l’ajout d’un chapitre sur la qualification des prestataires de certification électronique, d’horodatage électronique et d’audit de la sécurité des systèmes d’information.
Les administrations peuvent désormais recourir à des audits réalisés par des prestataires d’audit de la sécurité des systèmes d’information (PASSI) et ces derniers peuvent obtenir une qualification de leurs services.

Les annexes techniques ont été revues dans le même sens. “Certaines règles techniques concernant la cryptographie et la gestion des certificats électroniques ont également été adaptées pour en rendre l’application plus aisée”, précise l’Anssi, qui renvoie aussi au tout récent guide d’homologation, paru en juin.

« Un bon point de départ » – La V1 était une costaude introduction aux enjeux de la sécurité de l’e-administration et aux outils à mettre en œuvre : authentification, signature électronique, confidentialité, horodatage.

“Le RGS est le bon point de départ pour une collectivité qui se demande par où commencer. Mais il faut reconnaître que ce document n’est pas facile à lire pour quelqu’un qui n’est pas spécialisé dans la matière, il y a forcément besoin de se faire accompagner dans la mise en œuvre. Malgré tout, elle peut se faire pour des coûts modestes”, nous indiquait alors Marc Dovero, responsable de la sécurité des systèmes d’information (RSSI) du conseil général des Bouches-du-Rhône, département pilote pour

l'élaboration du RGS. "Il n'est pas facile d'accès", reconnaissait aussi Pierre Raynal, délégué de l'*OzSSI* Sud Est, qui précisait : "l'Anssi devait le faire pour démystifier le sujet."

Pas facile d'accès, et d'un niveau assez élevé, jugeait Yvonne Gellon, DSI de Grenoble Métropole, et présidente du CoTer Club, une association regroupant des collectivités territoriales dédiée à l'informatique et à la communication : "Si vous trouvez une collectivité conforme au RGS, je vous paye une bouteille ! Peut-être le Sictiam… ». Le Syndicat intercommunal des collectivités territoriales informatisées des Alpes méditerranée est un cas un peu particulier, puisqu'il a été précurseur du RGS, en travaillant avant sa création avec l'Anssi. Les DSI de l'agglomération de Grenoble se retrouvent régulièrement et avaient eu une formation de l'OzSSI. Ils ont ensuite effectué une analyse de risque préalable à sa mise en œuvre. "Sur toute l'agglomération, pas une collectivité n'est conforme. Mais c'est un outil qui a le mérite d'exister, de réglementer. C'est assez technique si on veut faire de la sécurité. C'est encore plus difficile à mettre en œuvre pour les petites. Il y a matière à simplifier les outils", indiquait-elle encore.

Limites de la vulgarisation – Cette V2 demande encore des efforts mais la vulgarisation sur certains sujets touche peut-être aussi ses limites, dans un contexte général de technicisation. On trouve donc encore des passages un peu rebutants, par exemple : « De ce fait, une signature électronique sécurisée au sens de l'article 1er du décret n° 2001-272 du 30 mars 2001, établie avec un dispositif sécurisé de création de signature certifié conforme dans les conditions de l'article 3 et mettant en œuvre des certificats de signature électronique conformes au niveau de sécurité (***) de [RGS_A2], est de facto « présumée fiable » selon ce décret et donc au sens de l'article 1316-4 du code civil."
Et reste que l'enjeu de la sécurité dans les collectivités ne semble pas vraiment la priorité de l'Anssi, si l'on en croit le programme de ses assises qui se tiennent cette semaine (voir ci-dessous).

Focus
Des assises de l'Anssi sans les collectivités

Cette semaine se tiennent les Assises de la sécurité et des systèmes d'information, "événement référent le plus prisé de la scène professionnelle de la SSI." Mais les collectivités et de façon plus générale la sphère publique en sont quasiment absentes : rien dans les conférences, les tables rondes comptent la plupart du temps un intervenant d'une entreprise privée.

Focus
Transition

La transition entre la V1 et la V2 concernant les certificats et les contremarques de temps est précisée : "les certificats électroniques et les contremarques de temps conformes aux annexes de la version 1.0 du RGS pourront continuer à être émis jusqu'au 30 juin 2015 ; les autorités administratives devront accepter ces certificats électroniques et ces contremarques de temps pendant leur durée de vie, avec un maximum de trois ans ; les autorités administratives doivent accepter les certificats électroniques et les contremarques de temps conformes aux annexes de la version 2.0 du RGS à compter du 1er juillet 2015."

Références
Le RGS V2

DOCUMENT 2

Règlement européen sur la protection des données : ce qui change pour les professionnels

15 juin 2016 – cnil.fr

Le nouveau règlement européen sur la protection des données personnelles paru au journal officiel de l'Union européenne entrera en application le 25 mai 2018. L'adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique.

La réforme de la protection des données poursuit trois objectifs :

1. **Renforcer les droits des personnes**, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
2. **Responsabiliser les acteurs traitant des données** (responsables de traitement et sous-traitants) ;
3. **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

Un cadre juridique unifié pour l'ensemble de l'UE

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Un champ d'application étendu

Le critère du ciblage

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

La responsabilité des sous-traitants

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »

Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transnationaux.

Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement sera transnational – donc qu'il concernera les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernées seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

Par exemple, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État.

Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

Un renforcement des droits des personnes

Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.

Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

De nouveaux droits

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Une conformité basée sur la transparence et la responsabilisation

Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

Une clé de lecture : la protection des données dès la conception et par défaut (*privacy by design*)

Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (*accountability*).
La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- le DPO (délégué à la protection des données)
- les études d'impact sur la vie privée (EIVP)

Les « études d'impact sur la vie privée » (EIVP ou PIA)

Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.
En cas de risque élevé, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.
Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

Le Délégué à la Protection des données (*Data Protection Officer*)

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.
Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Des responsabilités partagées et précisées

Le règlement européen sur la protection des données vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations pesant sur les responsables de traitements et les sous-traitants.

Le représentant légal

C'est le point de contact de l'autorité. Il a mandat pour « être consulté en complément ou à la place du responsables de traitement sur toutes les questions relatives aux traitements. »

Le sous-traitant

Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability. Il a notamment une obligation de conseil auprès du responsables de traitement pour la conformité à certaines obligations du règlement (PIA, failles, sécurité, destruction des données, contribution aux audits).
Il est tenu de maintenir un registre et de désigner un DPO dans les mêmes conditions qu'un responsable de traitement.

Le cadre des transferts hors de l'Union mis à jour

Les responsables de traitement et les sous–traitants peuvent transférer des données hors UE seulement s'ils encadrent ces transferts avec des outils assurant un niveau de protection suffisant et appropriés des personnes.
Par ailleurs, les données transférées hors Union restent soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.
Ainsi, et hormis les transferts fondés sur une décision d'adéquation de la Commission Européenne, les responsables de traitement et les sous-traitants peuvent mettre en place :

- des règles d'entreprises contraignantes (BCR) ;
- des clauses contractuelles types approuvées par la Commission Européenne ;
- des clauses contractuelles adoptées par une autorité et approuvées par la Commission européenne.

De nouveaux outils sont également prévus :

- pour les sous-traitants : la possibilité de mettre en place des règles d'entreprises contraignantes ;
- pour les autorités publiques : le recours à des accords contraignants ;

- pour les responsables de traitement et les sous-traitants : l'adhésion à des codes de conduite ou à un mécanisme de certification. Ces deux outils doivent contenir des engagements contraignants.

Enfin, une autorisation spécifique de l'autorité de protection basée sur ces outils n'est plus requise.

Des sanctions encadrées, graduées et renforcées

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

Les autorités de protection peuvent notamment :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Ce montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement pour le territoire de toute l'Union européenne.

Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de protection sera infligée à l'entreprise.

Comment les autorités de protection se préparent-elles ?

Le G29

Dans son plan d'action 2016, adopté en février 2016, le G29 a présenté ses priorités pour permettre l'application effective du règlement en avril 2018. Plusieurs groupes de travail se sont déjà mis en place pour décliner ce plan d'action.

Les 4 objectifs principaux :

1. Préparer la mise en place du Comité européen de la protection des données (CEPD), qui remplacera le G29 en 2018 ;
2. Préparer la mise en place du guichet unique et le mécanisme coopération et de cohérence entre les autorités ;
3. Proposer des lignes directrices ou des bonnes pratiques aux professionnels pour les 4 sujets prioritaires identifiés : le droit à la portabilité, la certification, le délégué à la protection des données (DPO), les traitements à risque d'ici la fin de 2016 ;
4. Promouvoir et diffuser le règlement afin que l'ensemble des acteurs se l'approprie.

Le G29 prévoit également la consultation régulière des parties prenantes dans une démarche itérative sur deux ans afin d'enrichir sa réflexion.

Il a organisé le 26 juillet 2016 à Bruxelles des ateliers collaboratifs. Cet espace de concertation multi-acteurs a réuni les représentants de la société civile, des fédérations professionnelles, des universitaires et des institutions européennes, autorités de protection des données autour des 4 sujets prioritaires qu'il a identifiés.
Les échanges et propositions de cette journée ont permis au G29 d'alimenter les différents groupes de travail qu'il a déjà mis en place autour de ces mêmes thèmes. L'objectif étant de décliner d'ici 2018 les principes du règlement en mesures opérationnelles correspondant aux besoins et attentes des principaux acteurs concernés par la mise en œuvre du règlement.
D'autres consultations seront organisées sur d'autres thématiques.

La CNIL

La CNIL est très impliquée dans chacun des groupes de travail mis en place par le G29, dont elle assure la Présidence jusqu'en février 2018.
Elle a proposé une consultation en ligne des acteurs français sur ces mêmes sujets.

DOCUMENT 3

Sécurité informatique

Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance

Publié le 23/02/2017 • par Pierre-Alexandre Conte • dans : Dossiers d'actualité, France • lagazettedescommunes.com


Apinan – Fotolia

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Chiffres-clés

Date clé : 4 mai 2018. C'est la date à laquelle le règlement européen sur la protection des données personnelles entrera en application. Ses objectifs ? Renforcer les droits des personnes, responsabiliser les acteurs traitant des données et crédibiliser la régulation. Les sanctions seront renforcées en cas de manquement à la loi. Les amendes pourront, par exemple, s'élever à 20 millions d'euros pour les collectivités.

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société. Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

Focus

50 % : Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces

objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »
Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.
« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.
La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.
« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

Focus

Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.
290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.
Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un

« ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

Focus

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

Références

- Guide d'homologation des systèmes d'information (Anssi)
- Référentiel général de sécurité (RGS)
- Guide d'hygiène informatique

DOCUMENT 4

ISO/CEI 27001

wikipedia.org – mis à jour le 21 août 2017

L'**ISO/CEI 27001** est une norme internationale de système de gestion de la sécurité de l'information de l'ISO et la CEI. Publiée en octobre 2005 et révisée en 2013, son titre est *"Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences"*. Elle fait partie de la suite ISO/CEI 27000.
Dans sa version 2013, l'ISO 27001 est conforme à la nouvelle structure commune des normes de management de l'ISO, l'HLS (HLS : High Level Structure)[1].

Sommaire

Objectifs

La norme ISO 27001, publiée en octobre 2005 et révisée en 2013, succède à la norme BS 7799-2 de BSI (*British Standards Institution*)[2]. Elle s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…) La norme ISO/CEI 27001 décrit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI). Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisme. L'objectif est de protéger les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique. Cela apportera la confiance des parties prenantes.
La norme précise que les exigences en matières de mesures de sécurité doivent être adéquates et proportionnées aux risques encourus et donc ne pas être ni trop laxistes ni trop sévères.

L'ISO/CEI 27001 énumère un ensemble de points de contrôles à respecter pour s'assurer de la pertinence du SMSI, permettre de l'exploiter et de le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 114 mesures de sécurité de la norme ISO/CEI 27002 (anciennement ISO/CEI 17799), classées dans 14 sections. Comme pour les normes ISO 9001 et ISO 14001, il est possible de se faire certifier ISO 27001.
Un point a disparu par rapport à la norme BS 7799-2, l'ISO 27001 n'incorpore plus l'amélioration de la compétitivité, des cash flow, de la profitabilité, le respect de la réglementation et l'image de marque.
La version 2013 ne fait plus explicitement allusion au PDCA (ou roue de Deming), elle utilise la formulation « établir, implémenter, maintenir, améliorer »[3].

La structure de la norme

La norme 27001 comporte 11 chapitres ; les exigences qu'ils contiennent doivent être respectées pour obtenir une certification.

Phase Plan

Fixe les objectifs du SMSI
La phase Plan du SMSI comprend 4 étapes :

Étape 1 : Définir la politique et le périmètre du SMSI

Périmètre : domaine d'application du SMSI. Son choix est libre, mais il est essentiel, car il figure ensuite le périmètre de certification. Il doit comprendre tous les actifs métiers (actifs primordiaux au sens de la norme ISO27005) et les actifs support à ces activités qui sont impliquées dans le SMSI.
Politique : niveau de sécurité (intégrité, confidentialité, disponibilité de l'information) qui sera pratiqué au sein de l'entreprise. La norme n'impose pas de niveau minimum de sécurité à atteindre dans le SMSI. Son niveau devant être proportionné aux risques évalués.
Le choix du périmètre et de la politique étant libre, ces deux éléments sont des « leviers de souveraineté » pour l'entreprise. Ainsi, une entreprise peut être certifiée ISO 27001 tout en définissant un périmètre très réduit et une politique de sécurité peu stricte et sans répondre aux exigences de ses clients en matière de sécurité.

Étape 2 : Identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité

La norme ISO 27001 ne donne pas de directives sur la méthode d'appréciation des risques à adopter. Les entreprises peuvent donc en inventer une en veillant à bien respecter le cahier des charges ou en choisir une parmi les plus courantes notamment la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) mise en place en France par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Le cahier des charges relatif à l'appréciation des risques se développe en 7 points :

1. Identifier les actifs
2. Identifier les personnes responsables
3. Identifier les vulnérabilités
4. Identifier les menaces
5. Identifier les impacts
6. Évaluer la vraisemblance
7. Estimer les niveaux de risque

Étape 3 : Traiter le risque et identifier le risque résiduel par un plan de gestion

Il existe quatre traitements possibles de chacun des risques identifiés :

1. L'acceptation (ou maintien) : ne mettre en place aucune mesure de sécurité supplémentaire car les conséquences de cette attaque sont acceptables (exemple :

vol d'un ordinateur portable ne comportant pas de données primordiales pour l'entreprise, piratage de la vitrine web…) Cette solution peut n'être que ponctuelle.

2. L'évitement : politique mise en place si l'incident est jugé inacceptable. L'évitement permet de sortir de la situation.
3. Le transfert (ou partage) : lorsque le risque ne peut pas être évité et qu'elle ne peut pas mettre en place les mesures de sécurité nécessaires elle transfère le risque par le biais de la souscription d'une assurance ou de l'appel à la sous-traitance par exemple.
4. La réduction : Réduire le risque à un niveau acceptable par la mise en œuvre de mesures techniques et organisationnelles, solution la plus utilisée.

Lorsque la décision de traitement du risque est prise, l'entreprise doit identifier les risques résiduels c'est-à-dire ceux qui persistent après la mise en place des mesures de sécurité. S'ils sont jugés inacceptables, il faut définir des mesures de sécurité supplémentaires. Cette phase d'acceptation formelle des risques résiduels s'inscrit souvent dans un processus d'homologation. Le système étant homologué en tenant compte de ces risques résiduels.

Étape 4 : Choisir les mesures de sécurité à mettre en place

La norme ISO 27001 contient une annexe A qui propose 114 mesures de sécurité classées en 14 catégories (politique de sécurité, sécurité du personnel, contrôle des accès…) Cette annexe normative n'est qu'une liste qui ne donne aucun conseil de mise en œuvre au sein de l'entreprise. Les mesures sont présentées dans la norme ISO 27002.

Phase Do

Met en place les objectifs

Elle se découpe en plusieurs étapes :

1. Établir un plan de traitement des risques
2. Déployer les mesures de sécurité
3. Générer des indicateurs
    - De performance pour savoir si les mesures de sécurité sont efficaces
    - De conformité qui permettent de savoir si le SMSI est conforme à ses spécifications
4. Former et sensibiliser le personnel

Phase Check

Consiste à gérer le SMSI au quotidien et à détecter les incidents en permanence pour y réagir rapidement.

Trois outils peuvent être mis en place pour détecter ces incidents :

1. Les audits internes qui vérifient la conformité et l'efficacité du système de management. Ces audits sont ponctuels et planifiés.
2. Le contrôle interne qui consiste à s'assurer en permanence que les processus fonctionnent normalement.
3. Les revues (ou réexamens) qui garantissent l'adéquation du SMSI avec son environnement.

Phase Act

Mettre en place des actions correctives, préventives ou d'amélioration pour les incidents et écarts constatés lors de la phase *Check*

- Actions correctives : agir sur les effets pour corriger les écarts puis sur les causes pour éviter que les incidents ne se reproduisent
- Actions préventives : agir sur les causes avant que l'incident ne se produise
- Actions d'amélioration : améliorer la performance d'un processus du SMSI.

Processus de certification

La certification n'est pas un but en soi, c'est-à-dire que l'organisme qui décide de mettre en place un SMSI en suivant les exigences de l'ISO 27001, n'a pas pour obligation de se faire certifier. Cependant, c'est l'aboutissement logique de l'implémentation d'un SMSI puisque les parties prenantes n'ont confiance qu'en un système certifié par un organisme indépendant.
La certification ISO 27001 se déroule sur un cycle de trois ans jalonné par l'audit initial, les audits de surveillance et l'audit de renouvellement.
L'audit initial porte sur l'ensemble du SMSI. Sa durée est déterminée dans l'annexe C de la norme ISO 27006. L'auditeur ne donne pas la certification, il donne juste un avis qui sera étudié par un comité de validation technique, puis par un comité de certification. Ce n'est qu'après cela que le certificat initial est délivré pour une durée de trois ans. Dans le cas contraire, il y a un audit complémentaire dans le délai maximum de trois mois. L'organisme devra, durant ce délai, corriger les problèmes décelés lors de l'audit initial pour obtenir le certificat.
L'audit de surveillance a lieu pendant la période de validité du certificat (3 ans) afin de s'assurer que le SMSI est toujours valable. Il y en a un par an. L'audit porte notamment sur les écarts ou non-conformités relevés lors de l'audit initial ainsi que sur d'autres points :

- le traitement des plaintes ;
- l'état d'avancement des activités planifiées ;
- la viabilité du SMSI ;
- l'utilisation de la marque de l'organisation certificatrice ;
- différentes clauses choisies par l'auditeur.

Si l'auditeur relève des non-conformités, le certificat sera suspendu voire annulé. L'organisme doit donc être perpétuellement mobilisé.
L'audit de renouvellement se déroule à l'échéance du certificat. Il porte sur les non-conformités du dernier audit de surveillance ainsi que sur la revue des rapports des audits de surveillance précédents et la revue des performances du SMSI sur la période.

Critique du standard

Avantages

- Une description pratique et détaillée de la mise en œuvre des objectifs et mesures de sécurité.
- Un audit régulier qui permet le suivi entre les risques initialement identifiés, les mesures prises et les risques nouveaux ou mis à jour, afin de mesurer l'efficacité des mesures prises.
- Sécurité :

1. Processus d'amélioration continue de la sécurité, donc le niveau de sécurité a plutôt tendance à croître.
2. Meilleure maîtrise des risques
3. Diminution de l'usage des mesures de sécurité qui ne servent pas.

- Une certification qui améliore la confiance avec les parties prenantes.
- Homogénéisation : c'est un référentiel international. Cela facilite les échanges, surtout pour les entreprises qui possèdent plusieurs sites.
- Processus simple et peu coûteux : réduction des coûts grâce à la diminution d'usage de mesures de sécurité inutiles et à la mutualisation des audits (baisse du nombre et de la durée des audits quand on obtient la certification).
- La norme fournit des indicateurs clairs et fiables ainsi que des éléments de pilotage financier aux directions générales.

- La norme permet d'identifier plus efficacement les risques et les coûts associés.

Limites

- Parfois, faible expérience des organismes d'accréditation par rapport aux spécificités des enjeux en sécurité des systèmes d'information.
- Relations commerciales prépondérantes (achat de certification, de conseil, de produits, de services), ce qui conduit à une dévalorisation du processus de certification.
- Durée courte pour les audits.
- La définition et la mise en place d'une méthodologie sont des tâches lourdes.
- L'application de cette norme ne réduit pas forcément de manière notable le risque en matière de piratage et de vols d'informations confidentielles. Les intervenants, notamment internes, connaissent les règles et peuvent ainsi plus aisément les contourner. Les normes sont inopérantes dans ce domaine.

Autour de la norme

Il existe toute une série de normes associées à l'ISO 27001, qui aident à la mise en place d'un SMSI.

ISO/CEI 27001 est, à l'origine, issue du standard britannique BS7799:2002 - Part 2.

Notes et références

1. « HLS: La structure universelle des normes de management » [archive], 18 novembre 2014
2. Norme ISO 27001 [archive] sur le site de BSI Group
3. « ISO 27001:2013, comparatif avec la version 2005 » [archive] [PDF], sur *club-27001.fr*, p. 5

Voir aussi

Bibliographie

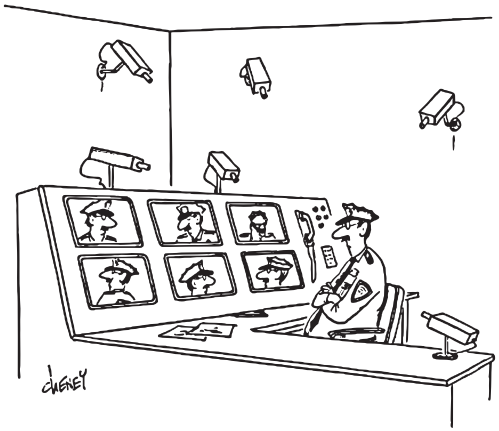
- Alexandre Fernandez-Toro, Management de la sécurité de l'information : implémentation ISO 27001 : mise en place d'un SMSI et audit de certification, Paris, Eyrolles, 2007

Articles connexes

- ISO/CEI 17799:2005
- Exigences
- Intelligence économique
- ITSEC
- Liste des normes ISO de la suite ISO/CEI 27000
- Liste de normes ISO par domaines
- Norme
- Sécurité de l'information
- Sécurité des systèmes d'information
- EBIOS, méthode de gestion des risques de l'ANSSI
- La dernière modification de cette page a été faite le 21 août 2017 à 14:46.

Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année



Méthodologie sécurité — P-F. Bonnefoi

Version du 10 avril 2017

Une affaire de standards

l'ISO, Organisation internationale de normalisation, «*International organization for standardization*»

- organisation internationale, créée en 1947 ;
- composée de représentants des organismes de normalisation nationaux d'environ 150 pays ;
- produit des normes internationales dans les domaines industriels et commerciaux.

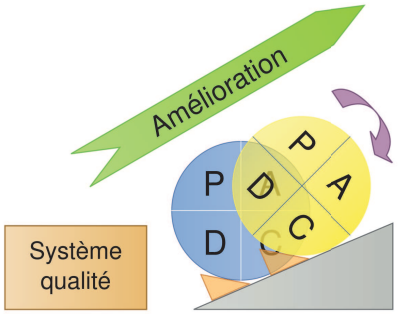
Différentes normes, IS, «*International Standard*» :

- IS 9000 : consacrée à la définition d'un «*système de management*» :
  - établir une politique et fixer des objectifs :
    - référentiel écrit ;
    - ensemble de mesures organisationnelles et techniques destinées à mettre en place un certain contexte organisationnel et à en assurer la pérennité et l'amélioration ;
  - vérifier que l'on a atteint les objectifs fixés :
    - réaliser un *audit* qui consistera à comparer le référentiel à la réalité pour relever les divergences, nommées *écarts* ou *non-conformités*.
    - sans référentiel, l'auditeur en peut réaliser sa mission ;
      mais il existe de nombreux référentiels…
- IS 9001 : consacrée aux systèmes de management de la qualité et aux exigences associées ;
- IS 14001 : consacrée aux systèmes de management de l'environnement ;
- IS 27001 : consacrée aux **systèmes de management de la sécurité de l'information** ;
- IS 19001 : directives à respecter pour la conduite de l'audit d'un système de management.

La norme ISO 27001

Système de management de la sécurité de l'information ou SMSI

- s'applique à un SMSI ;
- fournie un schéma de certification pouvant être appliqué au SMSI au moyen d'un audit ;
- s'appuie sur une approche *par processus* : exemple du PDCA, «*Plan, Do, Check, Act*» :



  - phase **Plan** :
    - définir le champ du SMSI,
    - identifier et évaluer les risques,
    - produire le document (*Statement of applicability*, SOA) qui énumère les mesures de sécurité à appliquer ;
  - phase **Do** :
    - affecter les ressources nécessaires,
    - rédiger la documentation,
    - former le personnel,
    - appliquer les mesures décidées,
    - identifier les risques résiduels ;
  - phase **Check** : audit et revue périodiques du SMSI, qui produisent des constats et permettent d'imaginer des corrections et des améliorations ;
  - phase **Act** :
    - prendre les mesures qui permettent de réaliser les corrections et les améliorations dont l'opportunité a été mise en lumière par la phase Check,
    - préparer une nouvelle itération de la phase Plan.

La norme ISO 27001

Le SMSI a pour buts de :

- **maintenir et d'améliorer la position** de l'organisme qui le met en œuvre du point de vue :
  - de la compétitivité,
  - de la profitabilité,
  - de la conformité aux lois et aux règlements,
  - de l'image de marque.
- **protéger les actifs «assets»** de l'organisme, définis au sens large comme *tout ce qui compte pour lui*.

Le vocabulaire du SMSI est fournie dans l'IS 27000.

Les mesures de sécurité énumérées dans la phase Plan peuvent être prises dans le **catalogue** de «mesures» et «bonnes pratiques» proposé par l'IS 27002.

Les méthodes d'analyse des risques

IS 27001 impose une **analyse des risques**, mais **ne propose aucune méthode** pour la réaliser :

- **liberté de choisir** une méthode pour le SMSI, à condition que :
  - elle soit documentée ;
  - elle garantisse que les évaluations réalisées avec son aide produisent des résultats **comparables** et **reproductibles**.

Exemples de méthodes d'analyse des risques :

- **IS 27005**, méthode d'analyse fournie par l'ISO ;
- **EBIOS®**, «*Expression des Besoins et Identification des Objectifs de Sécurité*» : méthode d'évaluation des risques en informatique, développée par l'**Agence nationale de la sécurité des systèmes d'information** (ANSSI).
- **MEHARI**, «*Méthode harmonisée d'analyse des risques*» : méthode visant à la sécurisation informatique d'une entreprise ou d'un organisme. Elle a été développée et est proposée par le **Club de la Sécurité de l'Information Français**, CLUSIF.

Pour obtenir une certification IS 27001

- définir le champ du SMSI ;
- en formuler la politique de management ;
- préciser la méthode d'analyse de risques utilisée ;
- identifier, analyser et évaluer les risques ;
- déterminer les traitements qui seront appliqués aux différents risques, ainsi que les moyens d'en vérifier les effets ;
- attester l'engagement de la direction de l'organisme dans la démarche du SMSI ;
- rédiger le *Statement of Applicability* (SOA) qui sera la charte du SMSI et qui permettra de le soumettre à un audit.

Les méthodes et l'aspect législatif

Les différents IS

- IS 27001 : système de management de la sécurité des systèmes d'information (SMSI) ;
- IS27000 : vocabulaire SSI ;
- IS 27002 : catalogue de mesures de sécurité : `https://fr.wikipedia.org/wiki/ISO/CEI_27002`
- IS 27003 : implémentation du SMSI ;
- IS 27004 : indicateurs de suivi du SMSI ;
- IS 27005 : évaluation et traitement du risque ;
- IS 27006 : certification du SMSI ;
- IS 27007 : audit du SMSI.

L'historique et l'évolution de la législation

- juillet 2002, USA : **loi Sarbanes-Oxley**, «*SOX*» : impose aux entreprises qui font appel au capital public (cotées en bourse) toute une série de règles comptables et administratives destinées à assurer la traçabilité de leurs opérations financières, pour garantir plus de transparence pour les actionnaires (éviter les comptes truqués comme dans le cas du scandale «Enron») ;
- 1er août 2003, France : **loi du sur la sécurité financière** (LSF) qui concerne principalement trois domaines :
  - modernisation des autorités de contrôle des marchés financiers ;
  - sécurité des épargnants et des assurés ;
  - contrôle légal des comptes ainsi que la transparence et le gouvernement d'entreprise. *Cette loi française ne concerne pas seulement les sociétés cotées, mais toutes les sociétés anonymes*.
- 2004, **dispositif réglementaire européen «Bâle 2»** qui concerne les établissements financiers.

La loi Sarbanes-Oxley concerne la sécurité du système d'information : elle impose aux entreprises des procédures de contrôle interne, de conservation des informations, et de garantie de leur exactitude :

- *la continuité des opérations ;*
- *la sauvegarde et l'archivage des données ;*
- *l'externalisation et son contrôle.*

Les normes par secteurs d'activité

Standards et référentiels à suivre afin d'assurer la sécurité de l'activité

- Secteur publique (Autorité administrative)
- Banque (CFONB, PCI-DSS, Bâle II)
- Assurance (Pack assurance, Solvabilité, CPR)
- Santé (HAS/DGOS, PSSIE, PGSSE_S, hôpital numérique) «*Haute Autorité de Santé/direction générale de l'Offre de soins*», «*Politique de sécurité des systèmes d'information de l'Etat*», «*Plan Générale de Santé, Sécurité et Environnement*»
- Industrie (Sevezo, CFR 21)
- Environnemental (ISO 14001) «Management environnemental»
- Alimentaire (ISO 22000) «Management de la sécurité des denrées alimentaires»
- Transaction web (21188 :2006) «Infrastructure de clé publique pour services financiers – Pratique et cadre politique»

Connaître, appliquer et respecter les normes qui s'appliquent aux différents secteurs d'activité de l'entreprise permet de se protéger contre les ***risques juridiques***.

Qu'est-ce qu'un système d'Information ?

Une définition du système d'information

« Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information »

1. Les enjeux de la sécurité des S.I.

a. Préambule

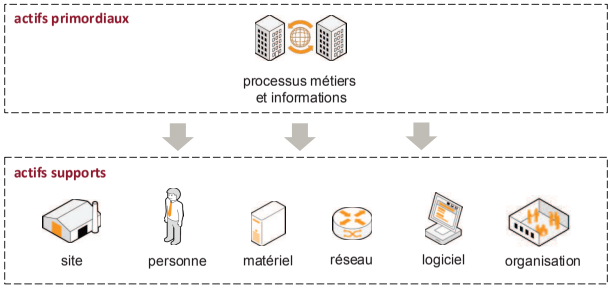
- Système d'Information (S.I.)
  - Ensemble des ressources destinées **à collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation
  - Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

Le S.I. doit permettre et faciliter la mission de l'organisation

1. Les enjeux de la sécurité des S.I.

a. Préambule

- Le système d'information d'une organisation contient un ensemble d'actifs :



ISO/IEC 27005:2008

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

1. Les enjeux de la sécurité des S.I.

b. Les enjeux

- La sécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations…
- La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :
  - Elle **contribue à la qualité de service que les utilisateurs** sont en droit d'attendre
  - Elle **garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

1. Les enjeux de la sécurité des S.I.

b. Les enjeux

1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- Les motivations évoluent
  - Années 80 et 90 : beaucoup de bidouilleurs enthousiastes
  - De nos jours : majoritairement des actions organisées et réfléchies

- Cyber délinquance
  - Les individus attirés par l'appât du gain
  - Les « hacktivistes »
  - Motivation politique, religieuse, etc.
  - Les concurrents directs de l'organisation visée
  - Les fonctionnaires au service d'un état
  - Les mercenaires agissant pour le compte de commanditaires
  - …

1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires

- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)

- **Chantage**
  - Déni de service
  - Modifications des données

- **Espionnage**
  - Industriel / concurrentiel
  - Étatique

- …

Qu'est-ce que la sécurité informatique ?

D'après Wikipedia

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information.

La sécurité informatique a pour objectif de **maintenir**, à **un niveau convenable** (défini par la direction générale), les garanties suivantes :

- **Disponibilité** : garantie que les entités autorisées ont accès à tout moment aux éléments considérés.
- **Intégrité** : garantie que les ressources sont exactes et complètes (non corrompues).
- **Confidentialité** : garantie que les ressources sont accessibles au moment voulu par les entités autorisées.
- **Tracabilité** : garantie que les accès et tentatives d'accès aux ressources sont tracés et que ces traces sont conservées et exploitables.

Ces quatre principes combinés, «*DICT*», permettent d'assurer un **niveau de sécurité suffisamment élevé** pour satisfaire au besoin de sécurité des données de l'entreprise concernée.

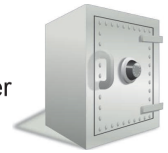
2. Les besoins de sécurité

a. Introduction aux critères DIC

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?

- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Bien à protéger



Disponibilité
Propriété d'accessibilité au moment voulu des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité
Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

Confidentialité
Propriété des biens de n'être accessibles qu'aux personnes autorisées

2. Les besoins de sécurité

b. Besoin de sécurité : « Preuve »

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?

- 1 critère complémentaire est souvent associé au D.I.C.

Bien à protéger

Preuve

Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe Notamment :

La traçabilité des actions menées
L'authentification des utilisateurs
L'imputabilité du responsable de l'action effectuée

2. Les besoins de sécurité

c. Exemple d'évaluation DICP

Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

L'expression du besoin attendu peut-être d'origine :

- **Interne** : inhérente au métier de l'entreprise
- ou **externe** : issue des contraintes légales qui pèsent sur les biens de l'entreprise.

Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :

Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible

Le bien bénéficie d'un niveau de sécurité adéquat

2. Les besoins de sécurité

c. Exemple d'évaluation DICP

- Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- Exemple avec un site institutionnel simple (statique) d'une entreprise qui souhaite promouvoir ses services sur internet :

Disponibilité = **Très fort**

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaitre ses services au public

Intégrité = **Très fort**

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)

Serveur web

Confidentialité = **Faible**

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = **Faible**

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

2. Les besoins de sécurité

d. Différences entre sureté et sécurité

« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements…

Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage…*

* Certaines de ces parades seront présentées dans ce cours

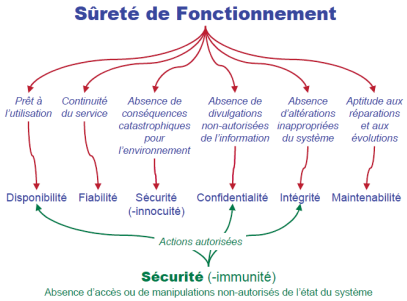
2. Les besoins de sécurité

d. Différences entre sureté et sécurité

Sûreté : ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.

Sécurité : ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

Le périmètre de chacune des 2 notions n'est pas si clairement délimité dans la réalité : dans le cas de la voiture connectée on cherchera la sécurité et la sûreté.



On constate sur le schéma que la notion de sécurité diffère selon le contexte :

- sécurité ▶ innocuité
- sécurité ▶ immunité

La méthode MEHARI «*Method for Harmonized Analysis of Risk*»

- ▷ méthode intégrée et complète d'évaluation et de management des risques visant à sécuriser les systèmes d'information d'une entreprise ou d'une organisation ;
- ▷ développée, diffusée et mise à jour par le club professionnel CLUSIF depuis 1996 ;
- ▷ mise à jour en 2010 pour respecter les lignes directrices de la norme ISO 27005 : 2009 ;
- ▷ utilisable dans le cadre d'un système de gestion de la sécurité de l'information de la norme ISO 27001 : 2005.

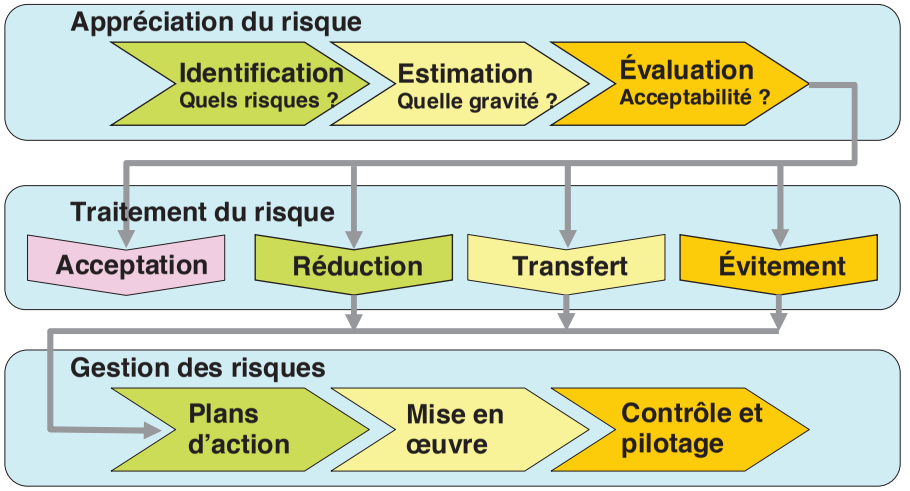
Une méthodologie en 3 étapes

I. l'**appréciation des risques** :
   a. identifier les risques du système d'information à partir d'une base de connaissance ;
   b. estimer la potentialité et l'impact de ces risques afin d'obtenir leur gravité
   c. évaluer l'acceptabilité ou non de ces risques.

II. le **traitement des risques** : prendre une décision pour chaque risque :
   - ◇ accepter
   - ◇ réduire
   - ◇ transférer
   - ◇ éviter.

III. la **gestion des risques** : établir des plans d'action de traitement des risques, des mises en œuvre de ces plans, mais aussi des contrôles et des pilotages de ces plans.

La méthode MEHARI «*Method for Harmonized Analysis of Risk*»



MÉthode Harmonisée d'Analyse des RIsques

Appréciation des risques

I. identifier tous les risques auxquels l'organisation est exposée ;
II. pour chacun des risques :
   - ◇ estimer sa **gravité** ;
   - ◇ juger de son acceptabilité.

> Attention
> *Tout risque ignoré ne sera l'objet d'aucune analyse ni d'aucun traitement.*

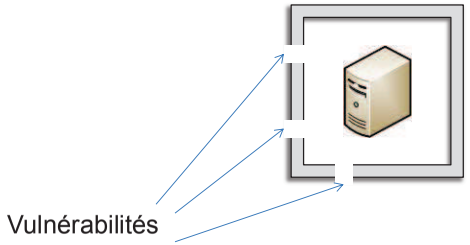
Identifier les risques

- ⋆ l'actif :
  - ◇ ce qui peut subir un **dommage** ;
  - ◇ le fait qu'un actif puisse subir un dommage crée un **risque** ;
  - ◇ la **gravité** associée à la survenance du risque **dépend de la nature** de cet actif ;
  - ◇ deux sortes d'actifs :
    - ⋆ **primaires** : les besoins de l'entreprise ;
    - ⋆ **secondaires**, ou «de support» : les différentes formes que peuvent prendre les actifs primaires.
- ⋆ la **vulnérabilité** : un actif peut posséder une ou plusieurs vulnérabilités intrinsèques qui entraîne des risques. Ces vulnérabilités dépendent du type d'*actif secondaire* (matériel, logiciel, *etc.*)
- ⋆ le **dommage subi** : exprimé suivant des **critères de conséquences** : disponibilité, intégrité et confidentialité.
- ⋆ la **menace** : cause d'exploitabilité (l'événement déclencheur) et une *probabilité d'occurence* d'un risque.

3. Notions de vulnérabilité, menace, attaque

a. Notion de « Vulnérabilité »

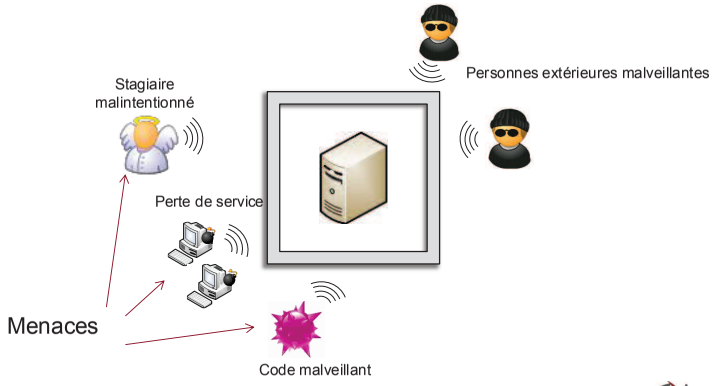
- **Vulnérabilité**
- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



3. Notions de vulnérabilité, menace, attaque

b. Notion de « Menace »

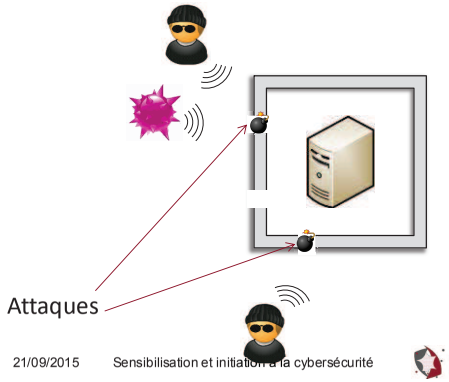
- **Menace**
- **Cause *potentielle* d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

- **Attaque**
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

- **Attaque**
- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maitriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

3. Notions de vulnérabilité, menace, attaque

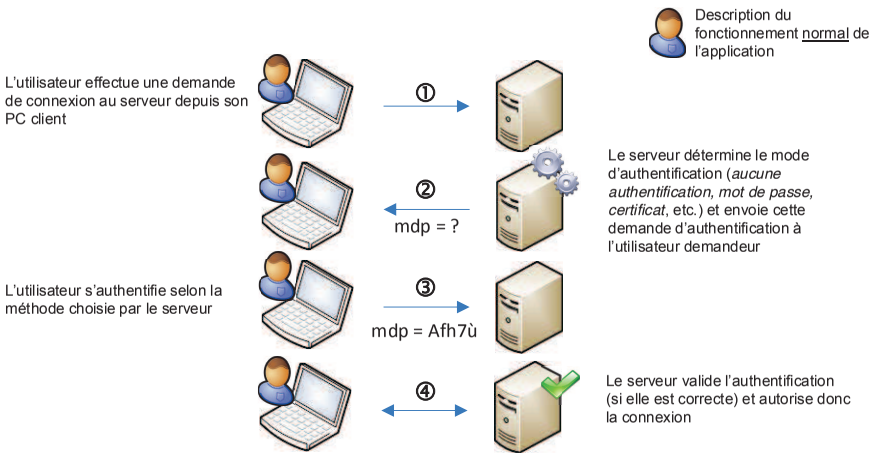
d. Exemple de vulnérabilité : Contournement de l'authentification dans l'application VNC

L'application VNC permet à un utilisateur de prendre en main sur une machine distance, après qu'il se soit authentifié.

- La vulnérabilité décrite dans les planches suivantes est corrigée depuis de nombreuses années. Elle est symptomatique d'une **vulnérabilité dans la conception d'une application ;**
- L'application permet en temps normal à un utilisateur de se connecter à distance sur une machine pour y effectuer un « partage de bureau » (i.e. pour travailler à distance sur cette machine) ;
- En 2006, il est découvert que cette application – utilisée partout dans le monde depuis de très nombreuses années – présente une vulnérabilité critique : il est possible de se connecter à distance sur cette application **sans avoir besoin de s'authentifier** (i.e. tout utilisateur sur internet peut se connecter à distance sur les systèmes en question) ;
- Le diaporama suivant illustre la **vulnérabilité technique** sous-jacente à ce comportement.

3. Notions de vulnérabilité, menace, attaque

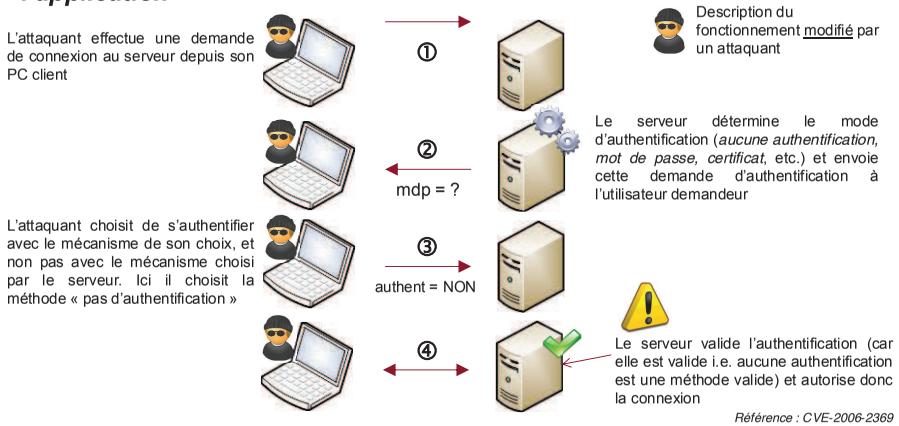
e. Illustration d'un usage normal de l'application vulnérable



Référence : CVE-2006-2369

3. Notions de vulnérabilité, menace, attaque

f. Illustration de l'exploitation de la vulnérabilité présente dans l'application



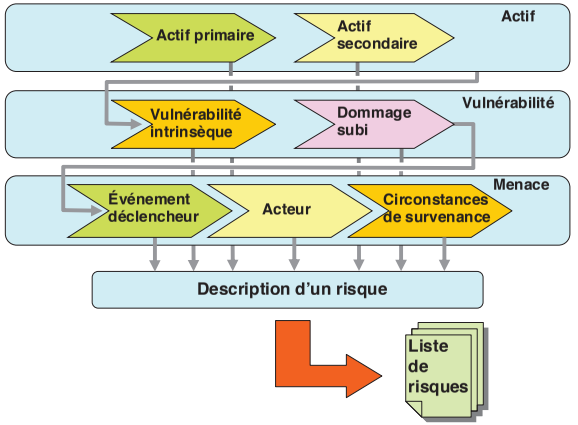
Référence : CVE-2006-2369

La vulnérabilité se situe ici : le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « authent = NON » est effectivement une authentification qui est toujours correcte)

Processus global d'élaboration des risques

▷ **Actifs primaires** *les besoins de l'entreprise* :
- ◇ services : informatiques, télécommunication, généraux ;
- ◇ données nécessaires au fonctionnement des services ;
- ◇ processus de gestion.

▷ **Actifs secondaires** *les diverses formes et contingences des actifs primaires* :
- ◇ moyens nécessaires à la réalisation des besoins fonctionnels décrits par les actifs primaires.



Un **risque** doit comprendre la description de l'actif en précisant l'actif primaire et secondaire.

Une **menace** comporte :
- ⋆ l'événement déclencheur et son caractère volontaire ou accidentel ;
- ⋆ l'acteur déclenchant cet événement ;
- ⋆ les circonstances dans lesquelles survient cet événement.

chacun de ces paramètres influe sur la probabilité d'occurrence de ce risque.

Exemples de risques, de scenarii et de préconisations : à la maison

Inventaire

Biens (maison, hi-fi, bijoux, ordinateur, etc.), personnes (famille, bébé, jeune enfant, etc.), animaux

Vulnérabilités/Services de sécurité

Porte, fenêtre, absence dans la journée ou les congés, présence de voisins, détecteurs incendie, etc.

Menaces

Cambriolage, incendie, inondation, etc.

Scénarii de risques

Incendie dans la chambre du bébé, vol avec effraction, etc.

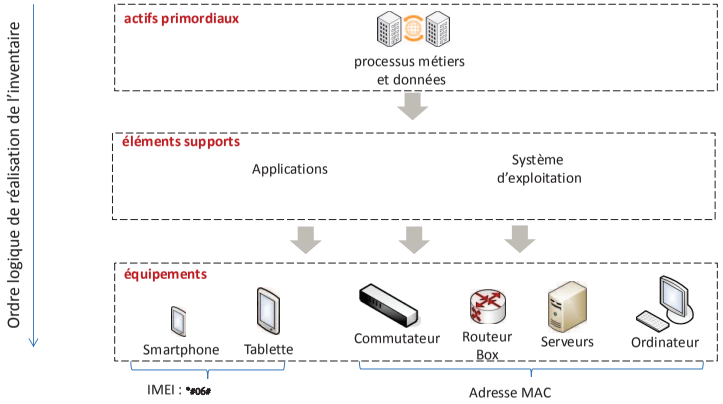
Préconisations

Mise en place de détecteurs de fumée, d'alarmes intrusion, etc.

1. Connaître le Système d'Information

a. Identifier les composants du S.I.

Différents éléments composent le SI



Comprendre son S.I. passe par l'identification de ses composants.

Actifs primaires & Secondaires

Primaires

Catégorie d'actifs : Services
Services du réseau étendu
Services du réseau local
Services applicatifs
Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)
Services systèmes communs : messagerie, archivage, impression, édition, etc.
Services d'interface et terminaux mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)
Services de publication d'informations sur un site web interne ou public
Services généraux de l'environnement de travail du personnel (bureaux, énergie, climatisation, etc.)
Services de télécommunication (voix, télécopies, visioconférence, etc.)

Secondaires

TYPES D'ACTIFS SECONDAIRES
Catégorie d'actifs : Services
Équipements matériels supports du service
Configurations logicielles
Media support de logiciel
Comptes et moyens nécessaires à l'accès au service
Services de sécurité associés au service
Moyens de servitude nécessaires au service
Locaux
Personnels et prestataires nécessaires pour le service (internes et externes)

Actifs primaires & Secondaires

Primaires

Catégorie d'actifs : Données
Fichiers de données ou bases de données applicatives
Fichiers bureautiques partagés
Fichiers bureautiques personnels (gérés dans un environnement personnel)
Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles
Listings ou états imprimés des applications informatiques
Données échangées, écrans applicatifs, données individuellement sensibles
Courrier électronique
Courrier postal et télécopies
Archives patrimoniales ou documentaires
Archives informatiques
Données et informations publiées sur un site web ou interne

Secondaires

Catégorie d'actifs : Données
Entités logiques : Fichiers ou bases de données
Entités logiques : Messages ou paquets de données en transit
Entités physiques : media et supports
Moyens d'accès aux données : clés et moyens divers, physiques ou logiques, nécessaires pour accéder aux données

Actifs primaires & Secondaires

Primaires

Catégorie d'actifs : Processus de management
Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels
Conformité à la loi ou aux réglementations relatives à la communication financière
Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée
Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle
Conformité à la loi relative à la protection des systèmes informatisés
Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement

Secondaires

Catégorie d'actifs : Processus de management
Procédures et directives internes (dispositifs organisationnels)
Moyens matériels nécessaires aux processus de management
Personnel et prestataires nécessaires aux processus de management

Estimation des risques

Pour estimer la gravité de chaque risque identifié, il faut tenir compte de :

- la gravité de risque **intrinsèque** (sans tenir compte des mesures de sécurité) ;
- la gravité de risque **résiduelle** (en tenant compte des mesures de sécurité).

Pour mesurer le risque, on utilise 2 paramètres :

- la probabilité ou la vraisemblance, appelée *potentialité*.
- la gravité des conséquences, appelé *impact*.

MEHARI fournit une échelle de potentialité et une échelle d'impact, standards à 4 niveaux.

La potentialité intrinsèque d'un risque

C'est la *probabilité maximale* de survenance du risque en l'absence de toute mesure de sécurité.
Elle dépend :

- de la localisation et de l'environnement de ce risque ;
- de l'enjeu d'un acte volontaire pour son auteur ;
- de la probabilité qu'une action volontaire vise précisément l'organisation.

Exemple : une entreprise de haute technologie est plus explosée au risque d'espionnage alors qu'une entreprise traitant des flux financiers est plus exposée aux tentatives de fraudes.

L'impact intrinsèque

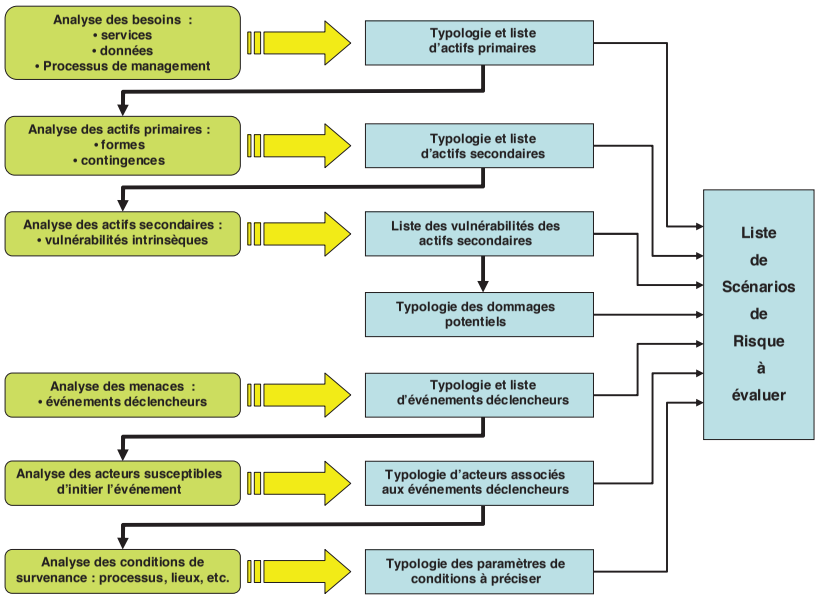
C'est le *niveau maximum* des conséquences possibles pour l'organisation en l'absence de toute mesure de sécurité.

Les mesures de sécurité

Ce sont des facteurs de *réduction des risques* :

- **Facteurs de réduction de potentialité** :
  - cumulables : empêcher totalement un événement de se produire, interdire une action humaine, *etc.*
  - deux types :
    - **Dissuasion** : rendre moins probable que l'acteur passe à l'action.
      Elle repose sur 3 principes :
      - l'imputabilité de l'action à son auteur ;
      - l'existence de sanctions ;
      - la connaissance par l'auteur des possibilités d'imputation et des sanctions.
    - **Prévention** : rendre moins probable que l'action aboutisse à la réalisation du risque : mesures techniques et de mécanismes de contrôle.
- **Facteurs de réduction d'impact** :
  - cumulables : limiter les conséquences directes possibles, prévoir la réparation d'un équipement suite à un sinistre, *etc.*
  - deux types :
    - **Confinement** : limiter l'ampleur des conséquences directes : fixation de limites telle que des limites physiques, fixation de points de contrôle intermédiaires, *etc.*
    - **Effet palliatif** : minimiser les conséquences indirectes du risque par une anticipation de la gestion du risque : plans de maintenance matérielle et logicielle, plans de sauvegarde et de restauration de données, *etc.*

Estimation des risques



Évaluation des risques dans MEHARI

MEHARI propose trois types de gravité de risque :

- les risques **insupportables** : ils doivent faire l'objet de mesure d'urgence.
- les risques **inadmissibles** : ils doivent être éliminés ou réduits à une échéance fixée.
- les risques **tolérés**.

Pour savoir dans quel type se range un risque, on :

- ▷ détermine sa gravité globale ;
- ▷ consulte la *Grille d'acceptabilité des risques*.

La **G**ravité globale d'un risque dépend de sa **P**otentialité et de son **I**mpact :

4	risque insupportable
3	risque inadmissible
1& 2	risque toléré.

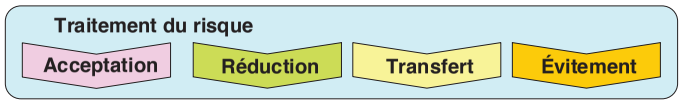
I = 4	G = 2	G = 3	G = 4	G = 4
I = 3	G = 2	G = 3	G = 3	G = 4
I = 2	G = 1	G = 2	G = 2	G = 3
I = 1	G = 1	G = 1	G = 1	G = 2
	P = 1	P = 2	P = 3	P = 4

L'utilisation d'une grille prédéterminée permet de :

- ▷ déterminer quelle décision prendre en terme « *d'acceptabilité du risque* » ;
- ▷ assurer la cohérence des décisions prises.

Traitement des risques

Les options principales conformes à la norme IS 27005



- ▷ **accepter** : l'entreprise accepte de rien faire vis-à-vis de cette situation :
  - ◇ le risque a été évalué comme acceptable dans la « grille d'acceptabilité des risques » ;
  - ◇ pour des raisons économiques, il a été jugé impossible d'y remédier ;
  - ◇ le risque est connu et sera surveillé dans le futur.
- ▷ **réduire** : sélectionner des services de sécurité dans une « **base de connaissance** » où chaque service est décrit avec
  - ◇ sa finalité/objectif ;
  - ◇ les mécanismes techniques/organisationnels pour sa mise en œuvre ;
  - ◇ un niveau de qualité suivant une échelle de niveau permettant de :
    - ⋆ donner une valeur globale lors de la combinaison de plusieurs services ;
    - ⋆ vérifier que le risque est ramené à un **niveau de gravité acceptable**.
- ▷ **transférer** : généralement en ayant recours à une assurance mais aussi en transférant la charge sur un tiers responsable par une action en justice.
- ▷ **éviter** : réduction par des mesures structurelles :
  - ◇ déménager en cas de risque d'inondation ;
  - ◇ limiter les encours disponibles en cas de risque de vol.

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie :

		D	I	C	P
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓	
Cryptographie	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓	✓
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓		✓	
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées		✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	

Gestion des risques

- ◦ intervient après les décisions de traitement de risques ;
- ◦ comprend l'ensemble des processus qui vont permettre de :
  - ◇ mettre en œuvre ces décisions ;
  - ◇ en contrôler les effets ;
  - ◇ les améliorer si nécessaire ;

Élaboration des plans d'action

- – mise en place de services de sécurité, avec, pour chacun, un objectif de niveau de qualité ;
- – mesures structurelles visant à réduire l'exposition à certains risques ;
- – mesures organisationnelles visant à éviter certains risques.

En raison de contraintes de budget, de personnels, toutes ces actions ne peuvent être entreprises immédiatement :

- ▷ choix des objectif prioritaires en terme de services de sécurité et optimisation de ce choix ;
- ▷ transformation de ces choix de services de sécurité en **plans d'action concrets** ;
- ▷ choix des mesures structurelles et des mesures d'évitement des risques ;
- ▷ **validation** des décisions précédentes.

Gestion des risques

Choix des objectifs prioritaires et optimisation

Pour définir les priorités, il faut tenir compte de :

- les niveaux de gravité des risques que les mesures prioritaires permettront de réduire : les risques de niveau le plus élevé doivent être traités en premier ;
- le nombre de risques traités et le nombre de risques dont le traitement sera remis à plus tard ;
- la rapidité avec laquelle les premiers résultats pourront être observés ;
- l'incidence de ces choix sur la sensibilisation du personnel ;
- *etc.*

Des outils informatiques d'optimisation peuvent aider à déterminer ces choix.

Choix des solutions : mécanismes techniques et organisationnels

Le choix revient au équipes et personnels spécialisés : DSI, «Direction des Systèmes d'Information», responsables réseaux, responsables de la sécurité physique, RSSI *etc.*

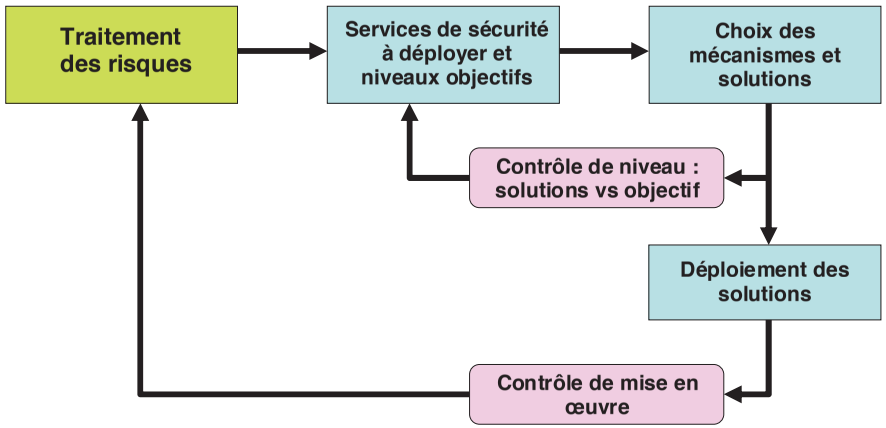
Regroupés dans un «*manuel de références des services de sécurité*», chaque service de sécurité :

- ☐ l'**objectif** du service ;
- ☐ les **résultats attendus** de la mise en œuvre du service ;
- ☐ la description des **mécanismes** associés à chaque service techniques et organisationnels ;
- ☐ les éléments permettant d'évaluer la **qualité** de chaque service :
  - ◇ efficacité ;
  - ◇ robustesse ;
  - ◇ mise sous contrôle ;

L'utilisation de ce manuel garantit la concordance entre les fonctionnalités attendues par les gestionnaires de risques et les estimations des facteurs de réduction de risques utilisées pour les sélectionner.

MEHARI propose un manuel de référence de services de sécurité.

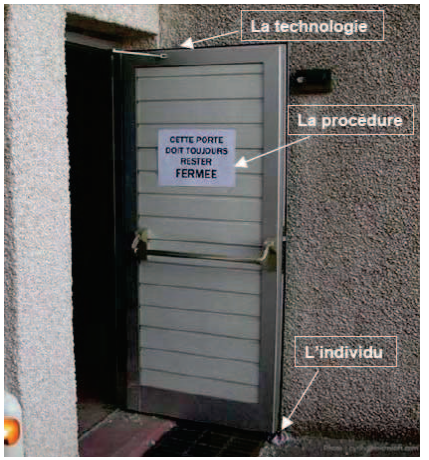
Contrôle et pilotage de la gestion directe des risques



Contrôle à effectuer :

- **premier niveau** : contrôler que les mécanismes et solutions de sécurité planifiés et décidés correspondent bien aux niveaux de qualité de service retenus en phase de traitement des risques ;
- **second niveau** : contrôler la mise en œuvre.

Gestion des risques : ne pas négliger le facteur humain !



La sécurité du système d'information dans l'entreprise

RSI
«*Responsable du Système d'Information*»

- ⋆ assure la gestion et l'exploitation du SI dont il a la responsabilité ;
- ⋆ connait tous les aspects aussi bien techniques, qu'organisationnels du SI dont il sert de personne de référence.

RSSI
«*Responsable de la Sécurité du SI*»

- ⋆ sécurise le SI afin de garantir :
  - ◇ disponibilité ;
  - ◇ intégrité ;
  - ◇ confidentialité ;
- ⋆ gère la sécurité au quotidien d'une manière globale, aussi bien technique qu'organisationnelle.

- ☐ PRA, «*plan de retour d'activité*» ;
- ☐ PCA, «*plan de continuité d'activité*» :
  - ◇ permet d'éviter une interruption de service qui engendrerait un PRA (reprise).
  - ◇ demande une surveillance pour fournir une continuité de service (outils de métrologie par exemple).
- ☐ SMSI, «Système de Management de la Sécurité de l'Information»
- ☐ PSSI, «Politique de Sécurité des Systèmes d'Information» : plan d'actions définies pour maintenir un certain niveau de sécurité.

PCA et PRA

PCA, «Plan de Continuité d'Activité»

But : **continuer** l'activité en cas d'incident ou de crise :
- ◇ sans perte de service ;
- ◇ avec une légère dégradation acceptable.

Exemple : *télétravail en cas de grève des transports en commun.*

PRA, «Plan de Reprise d'Activité»

But : **reconstruire** ou **basculer** sur un système de relève pour une durée déterminée en cas de crise majeure ou de sinistre :
- ◇ fournir les besions informatiques nécessaires à la survie de l'entreprise ;
- ◇ s'appui sur :
  - ⋆ RPO, «*Recovery Point Objective*», c-à-d un risque défini de perte de données ;
  - ⋆ RTO, «*Recovery Time Objective*», c-à-d une durée acceptable d'interruption.

Exemple : *basculement vers un «DataCenter» sur un site de secours en cas d'incendie.*

Des obligations

- ☐ Réglementation CRBF2004-02 (issue de IASB Bâle II) : obligation d'un plan de secours opérationnel pour les établissements financiers, banques et assurances.
- ☐ Code du commerce art. L.123-22 : conservation des documents comptables pendant 10 ans.
- ☐ Décret du 24 mars 2006 : conservation des fichiers de journalisation des prestataires d'hébergement (identification des personnes ayant édité du contenu mis en ligne).

Mise en œuvre d'un PCA/PRA ou «plan de secours»

Exemple d'une structure de formation

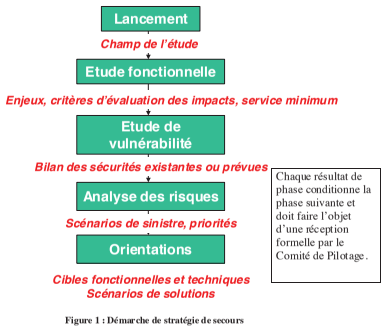


Figure 1 : Démarche de stratégie de secours

☐ **Lancement** :

Objectif : déterminer et préciser les risques à couvrir :
- ⋆ objets à risque : matériels informatiques et téléphoniques, fournisseurs extérieurs, personnels, locaux...
- ⋆ nature des risques.

Périmètre et risques :
- ⋆ limiter l'analyse au système informatique : serveurs et postes clients
- ⋆ exclure la situation de perte totale de données (productions et sauvegardes)

☐ **Étude fonctionnelle**

Objectif : activités qui exigent une continuité :
- ⋆ enjeux
- ⋆ activités essentielles
- ⋆ conséquences d'une interruption, dégradation : arrêt temporaire ou définitif, perte de données, dégradation de service...

Activités et exigences :

Étude du fonctionnement de la **structure de formation**

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Exemple d'une structure de formation

Quelles sont les activités qui exigent une continuité ?

Définir :
- ⋆ *les enjeux : permettre d'étalonner le niveau d'impact (caractère "non supportable") et de préciser les conditions minimales pour assurer un niveau d'activité et de disponibilité du SI acceptable.*
- ⋆ *les activités essentielles : les besoins informatiques en terme de process et de logiciels ;*
- ⋆ *les conséquences d'une interruption, dégradation (arrêt temporaire ou définitif, perte de données, dégradation de service..)*

Activités

a. un logiciel pour la **gestion des personnes inscrites** dans les différentes formations dispensées :
- ◇ inscription ;
- ◇ gestion des évaluations ;
- ◇ délivrance d'une attestion de suivi ou de réussite si la formation est diplômante ou fournie un certificat.

b. un logiciel de **gestion comptable** disposant d'une passerelle vers le logiciel de gestion des inscrits.

Exigences

Pour le logiciel a) :

élèves	temps d'arrêt max supportable
mai à juin	2 jours
septembre à octobre	2 jours
autres	3 jours

Pour le logiciel b) :

comptabilité	temps d'arrêt max supportable
janvier	1 jour
septembre à avril	2 jours
autres	4 jours

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Tableau récapitulatif du nombre de jours maximum d'interruption acceptable

mois	01	02	03	04	05	06	07	08	09	10	11	12
logiciel a) élèves	3	3	3	3	2	2	3	3	2	2	3	3
logiciel b) compta	1	2	2	2	3	3	3	3	2	2	2	2
maximum acceptable	1	2	2	2	2	2	3	3	2	2	2	2

Analyse

▷ Les logiciels d'exploitation se trouvant **sur le même serveur**, cela ramène la durée maximale d'interruption totale d'activité supportable à **deux jours sur toute l'année**.

*Si ce temps est ramené à une journée cela permet de limiter énormément le stress des **personnes concernées par l'utilisation de ce logiciel** et par conséquent, réduit le stress des **personnes qui s'occupent de la remise en activité du système**.*

▷ Ces deux jours concernent seulement la perte d'activité due au serveur.

La perte d'une journée de travail est le **maximum pour les périodes de forte activité**.
S'il y a perte totale de données, le coût devient très élevé car il faut reprendre les données en cours mais également reconstituer un historique minimum pour répondre à la législation (comptabilité, apprenants...)

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

- **Étude de vulnérabilité** :
  - Couverture assurance des risques informatiques : souscription d'une assurance couvrant les dégâts matériels et qui prévoit une indemnisation pour la reconstitution des données.
  - Sécurité générale : accès protégé aux serveurs, sauvegardes sur bandes.
  - Moyens de secours : pas de redondance de serveurs.
  - Moyens de protections des informations stockées : la bande magnétique de sauvegarde du vendredi sort du bâtiment.
    Elle n'est probablement pas chiffrée.
  - Contrats de maintenance : pour le serveur et les postes clients, imprimantes...
  - Sécurité du réseau informatique : utilisation d'un parefeu/firewall.

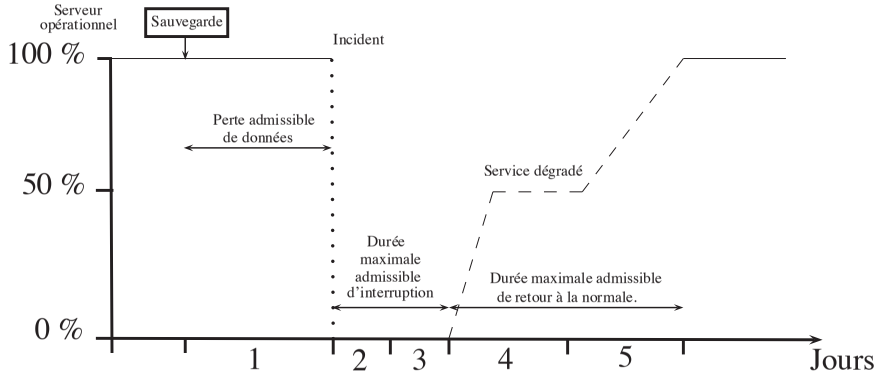
- **Analyse des risques**
  Les principaux risques pour les structures sont les
  - risques externes (force majeure) : électricité, incendie, dégâts des eaux, accès internet du FAI, vandalisme...
    Pour les risques électriques et d'incendie, les écoles accueillant du public sont contrôlées régulièrement avec des normes strictes. Les cas de forces majeures peuvent entraîner un arrêt complet si les serveurs sont tous sur le même site.
  - risques internes : le matériel, la mauvaise manipulation...

- **Orientations**
  Les solutions techniques et organisationnelles.

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Synthèse



Ressources disponibles

https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf
http://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-_sgdsn.pdf

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Orientations : quelques solutions

- ◯ Utiliser un **hébergeur externe** pour l'hébergement d'un site Web ;
  L'hébergeur doit disposer de son propre PCA/PRA.
- ◯ Héberger ses **applications métiers dans le Cloud** : Amazon Elastic Compute Cloud (EC2), etc.
  Si l'application métier a été adaptée à ce mode fonctionnement.
- ◯ **Sauvegarder régulièrement** en ligne ses données : GoogleDrive, DropBox, WEBdav...
  Disponible gratuitement pour les particuliers, à mettre en conformité avec la politique de sécurité de l'entreprise pour des données professionnelles, ou souscrire à une offre professionnelle.
- ◯ **Virtualiser** le poste de travail : VMWare, VirtualBox...
  Le matériel est interchangeable, seule compte la «machine virtuelle», qui se réduit à des fichiers représentant son disque dur. Par contre, bénéficie mal des performances des cartes graphiques.
- ◯ Stocker ses données sur un **serveur dans le réseau** : NAS, SAN...
  Le serveur n'héberge que des disques durs en mode RAID : survivre à la mort d'un des disques durs.
- ◯ Disposer **d'image complète** de son poste de travail : Clonezilla, Symantec Ghost...
  Permet de restaurer la totalité du disque dur de la machine, système d'exploitation et application compris.
- ◯ Utiliser des **applications disponible sur le Web** : Google Docs, Microsoft Office 365.
  Utiliser les solutions proposées par les éditeurs en matière de traitement de texte, de tableur et disposer de moyens de travail collaboratif.
- ◯ **Télétravail**.
  Permet de s'affranchir des risques liés aux retards et impossibilités de déplacement professionnels. Cela s'étend à l'usage de la visio conférence en lieu et place de déplacement de travail.

COMPLÉMENT

DOCUMENT 6

Numérique

Sécurité informatique : les collectivités territoriales, des cibles qui s'ignorent

Publié le 18/03/2016 • Par Pierre-Alexandre Conte • dans : France • lagazettedescommunes.com

Flickr CC by sa Sarah Joy

Les collectivités territoriales n'ont pas encore pris conscience de la nécessité de sécuriser leur système d'information, alors même qu'elles sont des cibles potentielles. C'est le constat dressé par l'ensemble des intervenants du colloque organisé mercredi 16 mars par la Mission Ecoter, « Criticité des données, cybersécurité : comment anticiper les risques, évaluer, s'assurer ? »

« Avant ce colloque, j'avais confiance en ma commune, mon conseil départemental ou régional. Aujourd'hui, je n'ai plus confiance en personne car je m'aperçois qu'on ne se préoccupe pas de mes données dans les collectivités territoriales », s'exclame Patrick Belin. Une affirmation empreinte d'ironie, lancée par le conseiller technique de la Mission Ecoter en conclusion du colloque organisé mercredi 16 mars sur le thème « Criticité des données, cybersécurité : comment anticiper les risques, évaluer, s'assurer ? » Une provocation gentille qui résume malgré tout assez bien les propos tenus au cours de l'événement. A l'issue de celui-ci, une idée ressortait en effet clairement : les collectivités territoriales ne sont en rien prêtes à faire face au danger qu'elles encourent.

« Un décalage entre la conscience et l'action concrète »

Le colloque s'est ouvert sur l'intervention de Gérard Combe. Le président de Primo France, une association dédiée à la gouvernance et à la gestion du risque public, a détaillé les résultats d'une étude menée en septembre 2015 auprès d'une centaine de communes portant sur l'exposition des villes au cyber risque et à ses conséquences.

Une série de sondages a permis de prendre conscience de l'ampleur du problème. Seulement 10% des villes interrogées ont déclaré organiser des formations pour sensibiliser leurs agents, moins de 15% ont admis ne pas avoir pris connaissance du Référentiel Général de Sécurité (RGS) de l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information), auquel les collectivités territoriales doivent se conformer depuis mai 2013 en ce qui concerne les certificats électroniques. Aucune d'entre elles n'a eu recours au chiffrement des données.

« Il y a une conscience du risque au quotidien mais il y a un décalage entre cette conscience et l'action concrète », affirme Gérard Combe. Un constat partagé par Jean-Pierre Soler,

directeur nouvelles technologies de la communauté d'agglomération Seine Essonne : « Trop peu de responsables sont conscients des failles de sécurité et de leurs infrastructures. » Avant de renchérir :
Je peux vous dire que l'on est mal vu dans les collectivités territoriales lorsque l'on met en place des procédures de sécurité. Passer de quatre à treize caractères pour les mots de passe, changer ce dernier toutes les quatre semaines, ne pas laisser un ordinateur allumé plus de cinq minutes lorsque l'on n'est pas à son poste : ce sont des mesures qui passent mal parce que personne n'a l'impression d'être une cible.
Quant aux élus, Jean-Pierre Soler ne les épargne pas non plus, rappelant qu'il est toujours plus vendeur auprès des électeurs « de garnir la ville de fleurs ou de proposer une jolie décoration de Noël » plutôt que de dégager un budget pour la sécurité numérique car « cela ne se voit pas ».

Un éventail de solutions

A l'occasion du colloque, la Mission Ecoter avait convié deux représentants de sociétés spécialisées dans la sécurité numérique, i-Tracing et EMC, qui ont exposé diverses solutions existant sur le marché pour protéger ses données. A commencer par la réplication de ces dernières avec la possibilité de mettre en place un PCA (Plan de Continuité de l'Activité) ou un PRA (Plan de Reprise de l'Activité), qui permettent dans un cas comme dans l'autre de faire face à un souci majeur touchant le système d'information.
Les intervenants ont aussi pris le temps d'expliquer que les collectivités territoriales étaient bien des cibles potentielles d'attaques, contrairement à ce que beaucoup d'entre elles tendent à penser. Des offensives qui pourraient notamment déboucher sur la perte de données sensibles. Mais pas uniquement dans la mesure où les communes, départements et régions peuvent aussi servir de leviers pour toucher d'autres organismes.
Jean-Christophe Bréchard, consultant en gestion des risques numériques et protection financière, a pour sa part rappelé l'existence d'assurances offrant une couverture globale, dès lors qu'il y a préjudice. « Trop souvent, a-t-il rappelé, l'assurance ne se met en route que lorsqu'une personne extérieure à l'affaire se manifeste. Or, ceux qui ont subi le préjudice doivent, dans de nombreux cas, débourser de l'argent pour prévenir les administrés ou les clients mais aussi faire venir des experts, etc.»

Homologuer son système d'information

Pour anticiper les problèmes, l'ANSSI a mis en place une démarche d'homologation en neuf étapes permettant aux collectivités territoriales de sécuriser leurs systèmes d'information. Un processus généralement assez lourd qui doit impérativement être adapté aux enjeux, au contexte d'emploi, à la nature des données et aux utilisateurs. Certains voudraient le généraliser, comme Jean-Pierre Soler, qui a enjoint l'ANSSI à utiliser de manière répétée « son fort pouvoir de coercition », pour contraindre les collectivités territoriales à « effectuer des audits » afin d'évaluer le degré de sécurité de leur système d'information.

19 Segmenter le réseau et mettre en place un cloisonnement entre ces zones

/STANDARD

Lorsque le réseau est « à plat », sans aucun mécanisme de cloisonnement, chaque machine du réseau peut accéder à n'importe quelle autre machine. La compromission de l'une d'elles met alors en péril l'ensemble des machines connectées. Un attaquant peut ainsi compromettre un poste utilisateur et ensuite « rebondir » jusqu'à des serveurs critiques.

Il est donc important, dès la conception de l'architecture réseau, de raisonner par segmentation en zones composées de systèmes ayant des besoins de sécurité homogènes. On pourra par exemple regrouper distinctement des serveurs d'infrastructure, des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, etc.

Une zone se caractérise alors par des VLAN et des sous-réseaux IP dédiés voire par des infrastructures dédiées selon sa criticité. Ainsi, des mesures de cloisonnement telles qu'un filtrage IP à l'aide d'un pare-feu peuvent être mises en place entre les différentes zones. On veillera en particulier à cloisonner autant que possible les équipements et flux associés aux tâches d'administration.

Pour les réseaux dont le cloisonnement a posteriori ne serait pas aisé, il est recommandé d'intégrer cette démarche dans toute nouvelle extension du réseau ou à l'occasion d'un renouvellement d'équipements.

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013

20 S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages

/STANDARD

L'usage du Wi-Fi en milieu professionnel est aujourd'hui démocratisé mais présente toujours des risques de sécurité bien spécifiques : faibles garanties en matière de disponibilité, pas de maîtrise de la zone de couverture pouvant mener à une attaque hors du périmètre géographique de l'entité, configuration par défaut des points d'accès peu sécurisée, etc.

La segmentation de l'architecture réseau doit permettre de limiter les conséquences d'une intrusion par voie radio à un périmètre déterminé du système d'information. Les flux en provenance des postes connectés au réseau d'accès Wi-Fi doivent donc être filtrés et restreints aux seuls flux nécessaires.

De plus, il est important d'avoir recours prioritairement à un chiffrement robuste (mode WPA2, algorithme AES CCMP) et à une authentification centralisée, si possible par certificats clients des machines.

La protection du réseau Wi-Fi par un mot de passe unique et partagé est déconseillée. À défaut, il doit être complexe et son renouvellement prévu mais il ne doit en aucun cas être diffusé à des tiers non autorisés.

Les points d'accès doivent par ailleurs être administrés de manière sécurisée (ex : interface dédiée, modification du mot de passe administrateur par défaut).

Enfin, toute connexion Wi-Fi de terminaux personnels ou visiteurs (ordinateurs portables, ordiphones) doit être séparée des connexions Wi-Fi des terminaux de l'entité (ex : SSID et VLAN distincts, accès Internet dédié).

ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi*, note technique, septembre 2013

21 Utiliser des protocoles réseaux sécurisés dès qu'ils existent

/STANDARD

Si aujourd'hui la sécurité n'est plus optionnelle, cela n'a pas toujours été le cas. C'est pourquoi de nombreux protocoles réseaux ont dû évoluer pour intégrer cette composante et répondre aux besoins de confidentialité et d'intégrité qu'impose l'échange de données. Les protocoles réseaux sécurisés doivent être utilisés dès que possible, que ce soit sur des réseaux publics (Internet par exemple) ou sur le réseau interne de l'entité.

Bien qu'il soit difficile d'en dresser une liste exhaustive, les protocoles les plus courants reposent sur l'utilisation de TLS et sont souvent identifiables par l'ajout de la lettre « s » (pour *secure* en anglais) à l'acronyme du protocole. Citons par exemple HTTPS pour la navigation Web ou IMAPS, SMTPS ou POP3S pour la messagerie.

D'autres protocoles ont été conçus de manière sécurisée dès la conception pour se substituer à d'anciens protocoles non sécurisés. Citons par exemple SSH (*Secure SHell*) venu remplacer les protocoles de communication historiques TELNET et RLOGIN.

ANSSI, *Recommandations pour un usage sécurisé d'[OPEN] SSH*, note technique, août 2016

22 Mettre en place une passerelle d'accès sécurisé à Internet

/STANDARD

L'accès à Internet, devenu indispensable, présente des risques importants : sites Web hébergeant du code malveillant, téléchargement de fichiers « toxiques » et, par conséquent, possible prise de contrôle du terminal, fuite de données sensibles, etc. Pour sécuriser cet usage, il est donc indispensable que les terminaux utilisateurs n'aient pas d'accès réseau direct à Internet.

C'est pourquoi il est recommandé de mettre en œuvre une passerelle sécurisée d'accès à Internet comprenant au minimum un pare-feu au plus près de l'accès Internet pour filtrer les connexions et un serveur mandataire (proxy) embarquant différents mécanismes de sécurité. Celui-ci assure notamment l'authentification des utilisateurs et la journalisation des requêtes.

/RENFORCÉ

Des mécanismes complémentaires sur le serveur mandataire pourront être activés selon les besoins de l'entité : analyse antivirus du contenu, filtrage par catégories d'URLs, etc. Le maintien en condition de sécurité des équipements de la passerelle est essentiel, il fera donc l'objet de procédures à respecter. Suivant le nombre de collaborateurs et le besoin de disponibilité, ces équipements pourront être redondés.

Par ailleurs, pour les terminaux utilisateurs, les résolutions DNS en direct de noms de domaines publics seront par défaut désactivées, celles-ci étant déléguées au serveur mandataire.

Enfin, il est fortement recommandé que les postes nomades établissent au préalable une connexion sécurisée au système d'information de l'entité pour naviguer de manière sécurisée sur le Web à travers la passerelle.

23 Cloisonner les services visibles depuis Internet du reste du système d'information

/STANDARD

Une entité peut choisir d'héberger en interne des services visibles sur Internet (site web, serveur de messagerie, etc.). Au regard de l'évolution et du perfectionnement des cyberattaques sur Internet, il est essentiel de garantir un haut niveau de protection de ce service avec des administrateurs compétents, formés de manière continue (à l'état de l'art des technologies en la matière) et disponibles. Dans le cas contraire, le recours à un hébergement externalisé auprès de professionnels est à privilégier.

De plus, les infrastructures d'hébergement Internet doivent être physiquement cloisonnées de toutes les infrastructures du système d'information qui n'ont pas vocation à être visibles depuis Internet.

Enfin, il convient de mettre en place une infrastructure d'interconnexion de ces services avec Internet permettant de filtrer les flux liés à ces services de manière distincte des autres flux de l'entité. Il s'agit également d'imposer le passage des flux entrants par un serveur mandataire inverse (*reverse proxy*) embarquant différents mécanismes de sécurité.

ANSSI, *Guide de définition d'une architecture de passerelle d'interconnexion sécurisée*, note technique, décembre 2011

ANSSI, *Maîtriser les risques de l'infogérance*, guide, décembre 2010

24 Protéger sa messagerie professionnelle

/STANDARD

La messagerie est le principal vecteur d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant.

Les utilisateurs doivent être particulièrement sensibilisés à ce sujet : l'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) est nécessaire.

Pour se prémunir d'escroqueries (ex : demande de virement frauduleux émanant vraisemblablement d'un dirigeant), des mesures organisationnelles doivent être appliquées strictement.

Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue une fuite irrémédiable d'informations de l'entité. Si nécessaire des moyens maîtrisés et sécurisés pour l'accès distant à la messagerie professionnelle doivent être proposés.

Que l'entité héberge ou fasse héberger son système de messagerie, elle doit s'assurer :

- de disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs pour prévenir la réception de fichiers infectés ;
- de l'activation du chiffrement TLS des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateur et les serveurs hébergeant les boîtes aux lettres.

/RENFORCÉ

Il est souhaitable de ne pas exposer directement les serveurs de boîte aux lettres sur Internet. Dans ce cas, un serveur relai dédié à l'envoi et à la réception des messages doit être mis en place en coupure d'Internet.

Alors que le spam - malveillant ou non - constitue la majorité des courriels échangés sur Internet, le déploiement d'un service anti-spam doit permettre d'éliminer cette source de risques.

Enfin, l'administrateur de messagerie s'assurera de la mise en place des mécanismes de vérification d'authenticité et de la bonne configuration des enregistrements DNS publics liés à son infrastructure de messagerie (MX, SPF, DKIM, DMARC).

ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*, guide, février 2015

25 Sécuriser les interconnexions réseau dédiées avec les partenaires

/STANDARD

Pour des besoins opérationnels, une entité peut être amenée à établir une interconnexion réseau dédiée avec un fournisseur ou un client (ex : infogérance, échange de données informatisées, flux monétiques, etc.).

Cette interconnexion peut se faire au travers d'un lien sur le réseau privé de l'entité ou directement sur Internet. Dans le second cas, il convient d'établir un tunnel site à site, de préférence IPsec, en respectant les préconisations de l'ANSSI.

Le partenaire étant considéré par défaut comme non sûr, il est indispensable d'effectuer un filtrage IP à l'aide d'un pare-feu au plus près de l'entrée des flux sur le réseau de l'entité. La matrice des flux (entrants et sortants) devra être réduite au juste besoin opérationnel, maintenue dans le temps et la configuration des équipements devra y être conforme.

/RENFORCÉ

Pour des entités ayant des besoins de sécurité plus exigeants, il conviendra de s'assurer que l'équipement de filtrage IP pour les connexions partenaires est dédié à cet usage. L'ajout d'un équipement de détection d'intrusions peut également constituer une bonne pratique.

Par ailleurs la connaissance d'un point de contact à jour chez le partenaire est nécessaire pour pouvoir réagir en cas d'incident de sécurité.

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, note technique, août 2015

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013

26 Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

/STANDARD

Les mécanismes de sécurité physique doivent faire partie intégrante de la sécurité des systèmes d'information et être à l'état de l'art afin de s'assurer qu'ils ne puissent pas être contournés aisément par un attaquant. Il convient donc d'identifier les mesures de sécurité physique adéquates et de sensibiliser continuellement les utilisateurs aux risques engendrés par le contournement des règles.

Les accès aux salles serveurs et aux locaux techniques doivent être contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge. Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont à proscrire, sauf s'il est possible de tracer strictement les accès et de limiter ces derniers en fonction des plages horaires. Une revue des droits d'accès doit être réalisée régulièrement afin d'identifier les accès non autorisés.

Lors du départ d'un collaborateur ou d'un changement de prestataire, il est nécessaire de procéder au retrait des droits d'accès ou au changement des codes d'accès.

Enfin, les prises réseau se trouvant dans des zones ouvertes au public (salle de réunion, hall d'accueil, couloirs, placards, etc.) doivent être restreintes ou désactivées afin d'empêcher un attaquant de gagner facilement l'accès au réseau de l'entreprise.

[...]

27 Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information

/STANDARD

Un poste de travail ou un serveur utilisé pour les actions d'administration ne doit en aucun cas avoir accès à Internet, en raison des risques que la navigation Web (à travers des sites contenant du code malveillant) et la messagerie (au travers de pièces jointes potentiellement vérolées) font peser sur son intégrité.

Pour les autres usages des administrateurs nécessitant Internet (consultation de documentation en ligne, de leur messagerie, etc.), il est recommandé de mettre à leur disposition un poste de travail distinct. À défaut, l'accès à une infrastructure virtualisée distante pour la bureautique depuis un poste d'administration est envisageable. La réciproque consistant à fournir un accès distant à une infrastructure d'administration depuis un poste bureautique est déconseillée car elle peut mener à une élévation de privilèges en cas de récupération des authentifiants d'administration.

/RENFORCÉ

Concernant les mises à jour logicielles des équipements administrés, elles doivent être récupérées depuis une source sûre (le site de l'éditeur par exemple), contrôlées puis transférées sur le poste ou le serveur utilisé pour l'administration et non connecté à Internet. Ce transfert peut être réalisé sur un support amovible dédié.

Pour des entités voulant automatiser certaines tâches, la mise en place d'une zone d'échanges est conseillée.

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, février 2015

42 Privilégier l'usage de produits et de services qualifiés par l'ANSSI

/RENFORCÉ

La qualification prononcée par l'ANSSI offre des garanties de sécurité et de confiance aux acheteurs de solutions listées dans les catalogues de produits et de prestataires de service qualifiés que publie l'agence.

Au-delà des entités soumises à réglementation, l'ANSSI encourage plus généralement l'ensemble des entreprises et administrations françaises à utiliser des produits qu'elle qualifie, seul gage d'une étude sérieuse et approfondie du fonctionnement technique de la solution et de son écosystème.

S'agissant des prestataires de service qualifiés, ce label permet de répondre aux enjeux et projets de cybersécurité pour l'ensemble du tissu économique français que l'ANSSI ne saurait adresser seule. Évalués sur des critères techniques et organisationnels, les prestataires qualifiés couvrent l'essentiel des métiers de la sécurité des systèmes d'information. Ainsi, en fonction de ses besoins et du maillage national, une entité pourra faire appel à un Prestataire d'audit de la sécurité des systèmes d'information (PASSI), un Prestataire de réponse aux incidents de sécurité (PRIS), un Prestataire de détection des incidents de sécurité (PDIS) ou à un prestataire de service d'informatique en nuage (SecNumCloud).

Catalogue des produits et prestataires de service qualifiés

I - Sensibiliser et former		STANDARD	RENFORCÉ
1	Former les équipes opérationnelles à la sécurité des systèmes d'information		
2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique		
3	Maîtriser les risques de l'infogérance		

II - Connaitre le système d'information		STANDARD	RENFORCÉ
4	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau		
5	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour		
6	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs		
7	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés		

III - Authentifier et contrôler les accès		STANDARD	RENFORCÉ
8	Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur		
9	Attribuer les bons droits sur les ressources sensibles du système d'information		
10	Définir et vérifier des règles de choix et de dimensionnement des mots de passe		
11	Protéger les mots de passe stockés sur les systèmes		
12	Changer les éléments d'authentification par défaut sur les équipements et services		
13	Privilégier lorsque c'est possible une authentification forte		

IV - Sécuriser les postes		STANDARD	RENFORCÉ
14	Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique		
15	Se protéger des menaces relatives à l'utilisation de supports amovibles		
16	Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité		

17	Activer et configurer le pare-feu local des postes de travail		
18	Chiffrer les données sensibles transmises par voie Internet		

V - Sécuriser le réseau		STANDARD	RENFORCÉ
19	Segmenter le réseau et mettre en place un cloisonnement entre ces zones		
20	S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages		
21	Utiliser des protocoles sécurisés dès qu'ils existent		
22	Mettre en place une passerelle d'accès sécurisé à Internet		
23	Cloisonner les services visibles depuis Internet du reste du système d'information		
24	Protéger sa messagerie professionnelle		
25	Sécuriser les interconnexions réseau dédiées avec les partenaires		
26	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques		

VI - Sécuriser l'administration		STANDARD	RENFORCÉ
27	Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information		
28	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information		
29	Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail		

VII - Gérer le nomadisme		STANDARD	RENFORCÉ
30	Prendre des mesures de sécurisation physique des terminaux nomades		
31	Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable		
32	Sécuriser la connexion réseau des postes utilisés en situation de nomadisme		
33	Adopter des politiques de sécurité dédiées aux terminaux mobiles		

VIII - Maintenir à jour le système d'information		STANDARD	RENFORCÉ
34	Définir une politique de mise à jour des composants du système d'information		
35	Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles		

IX - Superviser, auditer, réagir		STANDARD	RENFORCÉ
36	Activer et configurer les journaux des composants les plus importants		
37	Définir et appliquer une politique de sauvegarde des composants critiques		
38	Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées		
39	Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel		
40	Définir une procédure de gestion des incidents de sécurité		

X - Pour aller plus loin		STANDARD	RENFORCÉ
41	Mener une analyse de risques formelle		
42	Privilégier l'usage de produits et de services qualifiés par l'ANSSI		

[...]

DOCUMENT 8

Devenir délégué à la protection des données

23 mai 2017 – cnil.fr

Le délégué à la protection des données est au cœur du nouveau règlement européen. Les lignes directrices adoptées dans leur version finale le 5 avril 2017 par le G29, groupe des « CNIL » européennes, clarifient et illustrent d'exemples concrets le nouveau cadre juridique applicable en mai 2018 dans toute l'Europe.

Le règlement européen sur la protection des données pose les règles applicables à la désignation, à la fonction et aux missions du délégué, sous peine de sanctions.
Les lignes directrices du G29 ont pour objectif d'accompagner les responsables de traitement et les sous-traitants dans la mise en place de la fonction de délégué ainsi que d'assister ces délégués dans l'exercice de leurs missions. Elles contiennent des recommandations et des bonnes pratiques permettant aux professionnels de se préparer et de mettre en œuvre leurs obligations avec flexibilité et pragmatisme.
A la suite d'un appel à commentaires, les lignes directrices ont été enrichies et adoptées par le G29 dans leur version finale le 5 avril 2017.

A retenir
Le délégué est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.
Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.
Pour garantir l'effectivité de ses missions, le délégué :

- doit disposer de qualités professionnelles et de connaissances spécifiques,
- doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.

La mise en place de la fonction de délégué nécessite d'être anticipée et organisée dès aujourd'hui, afin d'être prêt en mai 2018.

Dans quels cas un organisme doit-il obligatoirement désigner un délégué à la protection des données ?

La désignation d'un délégué est obligatoire pour :

1. Les autorités ou les organismes publics,

2. Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors des cas de désignation obligatoire, la désignation d'un délégué à la protection des données est encouragée par les membres du G29. Elle permet en effet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles.

Les organismes peuvent désigner un délégué interne ou externe à leur structure. Le délégué à la protection des données peut par ailleurs être mutualisé c'est-à-dire désigné pour plusieurs organismes sous certaines conditions. Par exemple, lorsqu'un délégué est désigné pour un groupe d'entreprises, il doit être facilement joignable à partir de chaque lieu d'établissement. Il doit en effet être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec l'autorité de contrôle.

Les lignes directrices du G29 clarifient les critères posés par le règlement, notamment les notions d'autorité ou d'organisme public, d'activités de base, de grande échelle et de suivi régulier et systématique.

Quelles différences entre le CIL et le délégué ?

Le délégué à la protection des données est le successeur naturel du CIL. Leurs statuts sont similaires.

Toutefois, le règlement précise les exigences portant sur le délégué s'agissant de ses **qualifications** (qualités professionnelles, connaissances spécialisées du droit et des pratiques en matière de protection de données) et de sa **formation continue** (entretien de ses connaissances spécialisées).

Ses prérogatives et missions sont renforcées, s'agissant en particulier de son rôle de conseil et de sensibilisation sur les nouvelles obligations du règlement (notamment en matière de conseil et, le cas échéant, de vérification de l'exécution des analyses d'impact).

Par ailleurs, les organismes doivent fournir à leur délégué les ressources nécessaires à ses missions (notamment l'associer d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données, lui donner accès aux données ou encore lui permettre de se former).

Enfin, contrairement au CIL dont la désignation est facultative, celle du délégué est obligatoire dans certains cas (voir question ci-dessus).

Qui peut être délégué ?

Le délégué doit être désigné « *sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir [ses] missions* » (article 37.5 du règlement européen).

La personne qui a vocation à devenir délégué à la protection doit pouvoir réunir les qualités et compétences suivantes :

- l'aptitude à **communiquer efficacement** et à exercer ses fonctions et missions en **toute indépendance**. Le délégué ne doit pas avoir de **conflit d'intérêts** avec ses autres missions. Cela signifie qu'il ne peut occuper des fonctions, au sein de l'organisme, qui le conduise à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie ») (*voir la question spécifique sur le conflit d'intérêts*).

- une **expertise** en matière de **législations** et pratiques en matière de protection des données, acquise notamment grâce à une **formation continue**. Le niveau d'expertise doit être **adapté à l'activité** de l'organisme et à la **sensibilité** des traitements mis en œuvre.
- une **bonne connaissance** du secteur d'activité et de l'organisation de l'organisme et en particulier des **opérations de traitement**, des **systèmes d'information** et des **besoins** de l'organisme en matière de **protection** et de **sécurité** des données.
- un **positionnement efficace en interne** pour être en capacité de **faire directement rapport au niveau le plus élevé** de l'organisme et également **d'animer un réseau** de relais au sein des filiales d'un groupe par exemple et/ou une **équipe** d'experts en interne (expert informatique, juriste, expert en communication, traducteur, etc.).

Il n'existe donc **pas de profil type** du délégué qui peut être une personne issue du domaine technique, juridique ou autre. Une étude menée pour la CNIL en 2015 a en effet montré que les CIL proviennent de domaines d'expertise très variés (profil technique à 47%, profil juridique à 19% et profil administratif à 10%).

Attention : La mise en place de la fonction de délégué nécessite d'être anticipée et organisée dès aujourd'hui, afin d'être prêt en **mai 2018**.

Dans quel cas peut-il exister un conflit d'intérêts ?

La fonction de délégué peut être exercée à temps plein ou à temps partiel. Dans ce dernier cas, le délégué ne peut occuper des fonctions au sein de l'organisme le conduisant à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie »). L'existence d'un conflit d'intérêts est donc **appréciée au cas par cas**.

A titre d'exemple, les fonctions suivantes sont susceptibles de donner lieu à un conflit d'intérêts : secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique, mais également d'autres rôles à un niveau inférieur de la structure organisationnelle **si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement**. Un conflit d'intérêt peut également exister par exemple si un délégué sur la base d'un contrat de service représente l'organisme devant les tribunaux dans des dossiers impliquant des sujets en matière de données à caractère personnel.

Quelle est la responsabilité du délégué à la protection des données ?

La responsabilité du délégué est similaire à celle du CIL. Les lignes directrices du G29 précisent que **le délégué n'est pas responsable en cas de de non-respect du règlement**. Ce dernier établit clairement que c'est le responsable du traitement (RT) ou le sous-traitant (ST) qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions (article 24.1 du règlement). Le respect de la protection des données relève donc de la responsabilité du RT ou du ST.

Il n'est pas possible de transférer au Délégué, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant. En effet, cela reviendrait à conférer au Délégué un pouvoir décisionnel sur la finalité et les moyens du traitement ce qui serait constitutif d'un conflit d'intérêts contraire à l'article 38.6 du règlement européen.

En France, il existe des situations où le CIL (et le délégué) pourrait comme n'importe quel autre employé ou agent, voir sa **responsabilité pénale** engagée. Ainsi, la responsabilité pénale d'un CIL/délégué pourrait être retenue s'il enfreint intentionnellement les dispositions pénales de la loi Informatique et Libertés ou en tant que complice s'il aide le responsable du traitement ou le sous-traitant à enfreindre ces dispositions pénales.

Quelle protection pour le délégué à la protection des données ?

Le délégué doit agir d'une **manière indépendante** et bénéficier d'une **protection suffisante dans l'exercice de ses missions**. Le règlement prévoit ainsi que le délégué ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions.

Les sanctions ne sont pas possibles si elles sont imposées en raison de l'exercice par le délégué de sa fonction. A titre d'exemple, si un délégué estime qu'un traitement est susceptible d'engendrer un risque élevé et conseille au responsable de traitement de procéder à une analyse d'impact, et si le responsable de traitement n'est pas d'accord avec l'analyse du délégué, ce dernier ne peut être relevé de sa fonction pour avoir formulé ce conseil.

Les sanctions peuvent prendre des formes diverses et peuvent être directes ou indirectes. Il peut s'agir, par exemple, d'absence de promotion ou de retard dans la promotion, de freins à l'avancement de carrière ou du refus de l'octroi d'avantages dont bénéficient d'autres employés. Il n'est pas nécessaire que ces sanctions soient effectivement mises en œuvre, une simple menace suffit pour autant qu'elle soit utilisée pour sanctionner le délégué pour des motifs liés à ses activités en tant que délégué.

A noter toutefois que le délégué n'est pas un salarié protégé au sens du code du travail français. Dès lors, il pourrait être licencié légitimement, comme tout autre employé, pour des motifs autres que l'exercice de ses missions de délégué (par exemple, en cas de vol, de harcèlement physique, moral ou sexuel ou fautes graves similaires).

Où le délégué doit-il être localisé ?

Afin de permettre que le délégué soit joignable, il est recommandé qu'il soit localisé dans un Etat membre de l'Union européenne.

Toutefois, dans certaines situations où l'organisme n'a pas d'établissement dans l'Union européenne, un délégué peut être en mesure d'exercer ses missions plus efficacement s'il est localisé en dehors de l'Union européenne.

Quelles sont les missions du délégué à la protection des données ?

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- **d'informer et de conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- **de contrôler le respect du règlement** et du droit national en matière de protection des données ;
- **de conseiller l'organisme** sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci (voir question ci-après).

Les missions du délégué couvrent l'ensemble des traitements mis en œuvre par l'organisme qui l'a désigné.
Les lignes directrices détaillent le rôle du délégué en matière de contrôle, d'analyse d'impact et de tenue du registre des activités de traitement.
Elles indiquent que **le délégué n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement**.

Que signifie coopérer avec l'autorité de contrôle et être le point de contact avec celle-ci ?

L'une des missions du délégué est d'être le point de contact pour l'autorité de protection des données et de coopérer avec elle. A ce titre, le délégué doit faciliter l'accès par l'autorité aux documents et informations dans le cadre de l'exercice des missions et des pouvoirs de cette autorité (par exemple lors d'échanges avec l'autorité dans l'instruction d'une plainte, ou en cas besoin de précisions sur un projet en cours ou bien encore, dans le cadre d'un contrôle de l'autorité).
L'obligation de confidentialité ou de secret professionnel du délégué ne doit pas l'empêcher de demander conseil à l'autorité sur tout sujet, si nécessaire.

Quels sont les moyens d'action du délégué à la protection des données ?

Le délégué doit bénéficier du soutien de l'organisme qui le désigne. L'organisme devra en particulier :

- **s'assurer de son implication** dans toutes les questions relatives à la protection des données (exemple : communication interne et externe sur sa désignation)
- **lui fournir les ressources nécessaires** à la réalisation de ses tâches (exemples : formation, temps nécessaire, ressources financières, équipe)
- **lui permettre d'agir de manière indépendante** (exemples : positionnement hiérarchique adéquat, absence de sanction pour l'exercice de ses missions)
- **lui faciliter l'accès aux données et aux opérations de traitement** (exemple : accès facilité aux autres services de l'organisme)
- **veiller à l'absence de conflit d'intérêts**

Les lignes directrices fournissent des exemples concrets et opérationnels des ressources nécessaires à adapter selon la taille, la structure et l'activité de l'organisme. S'agissant du conflit d'intérêts, le délégué ne peut occuper des fonctions, au sein de l'organisme, qui le conduise à déterminer les finalités et les moyens d'un traitement (ne pas être juge et partie). L'existence d'un conflit d'intérêt est appréciée au cas par cas. Les lignes directrices indiquent les fonctions qui, en règle générale, sont susceptibles de conduire à une situation de conflit d'intérêts.

Quand et comment désigner un délégué à la protection des données ?

Un formulaire de désignation en ligne auprès de la CNIL devrait être disponible prochainement, cette désignation prenant effet le 25 mai 2018. Le contenu de ce formulaire est actuellement en cours d'élaboration.

Comment organiser la fonction de délégué à la protection des données ?

En vue de la préparation à la fonction de délégué, il est recommandé de :

- s'approprier les nouvelles obligations imposées par le règlement européen, en s'appuyant notamment sur les lignes directrices du G29 (portabilité, autorité chef de file, analyse d'impact).
- confier au CIL ou au futur délégué les missions suivantes :
    - **réaliser l'inventaire des traitements** de données personnelles mis en œuvre ;
    - **évaluer ses pratiques et mettre en place des procédures** (audits, *privacy by design*, notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
    - **identifier les risques** associés aux opérations de traitement ;
    - **établir une politique de protection des données personnelles** ;
    - **sensibiliser les opérationnels et la direction** sur les nouvelles obligations.

ANNEXE A

« Présentation du Système d'Information (SI) d'INGECO » – DSISN d'INGECO – 2018

Actuellement, il n'y a pas de mutualisation de la Direction des Systèmes d'Information et des Services Numériques (DSISN) pour l'ensemble des communes membres. Le développement et le maintien en condition opérationnelle du Système d'Information (SI) d'INGECO sont assurés par la DSISN.

Le SI comprend de nombreuses applications transversales (gestion financière, gestion des ressources humaines, gestion des délibérations ...) et des applications dédiées aux compétences de la collectivité (transports, développement économique ...).

Ces ressources sont majoritairement hébergées en interne mais certaines d'entre elles, comme la messagerie, les sites internet, ou quelques applications métiers sont hébergées dans le cloud, par des prestataires externes. De multiples applications contiennent des données personnelles. Les dossiers de consultation n'imposent pas de clauses particulières dans le domaine de la cybersécurité, hormis des préconisations d'ordre technique.

Le domaine de la cybersécurité est actuellement confié à la DSISN. Au sein de cette direction, ce sont différentes équipes qui gèrent la mise en place de solutions techniques, chacune dans leur domaine (réseau, systèmes, postes de travail, applications). Il n'y a pas de conduite d'audit de vulnérabilité.

Le rôle de Correspondant Informatique et Libertés (CIL) a été confié au directeur de la DSISN, personne n'ayant été volontaire pour assumer cette responsabilité.

La gestion de la cybersécurité ne fait l'objet d'aucun processus formalisé et ne mobilise aucune instance dédiée. Des actions de communication sont parfois menées sur l'intranet de la collectivité pour expliquer aux agents les raisons de la mise en œuvre de certaines contraintes (par exemple le changement régulier des mots de passe).

La métropole n'a jamais été la cible d'une cyberattaque. Les moyens financiers et humains consacrés à la cybersécurité sont en légère progression depuis 3 ans.