Sujet élaboré par une cellule pédagogique nationale

CONCOURS INTERNE D'INGÉNIEUR TERRITORIAL

SESSION 2019

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 lors de son inscription, au sein de la spécialité dans laquelle il concourt.

Durée : 8 heures
Coefficient : 7

SPÉCIALITÉ : INFORMATIQUE ET SYSTÈMES D'INFORMATION

OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

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 80 pages dont 2 annexes.

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.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- 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 (DSI) du département d'INGEDEP (2 500 agents) dont le Système d'Information (SI) a été victime récemment d'une cyber-attaque de type « Ransomware » de gravité moyenne et sans conséquence majeure.
Conscient de l'évolution des menaces en matière de cybersécurité, le Directeur des Systèmes d'Information (DSI) s'engage dans un projet global d'audit et de renforcement du niveau de sécurité du SI. Par ailleurs, la direction générale s'interroge sur les nombreux investissements réalisés dans le domaine de la sécurité du SI et sur la continuité d'activité de la collectivité en cas de sinistre.

À l'aide des annexes, vous répondrez aux questions suivantes :

Question 1 (5 points)

Différentes solutions de sécurité ont été mises en place et le DSI s'interroge sur l'empilement de ces solutions techniques et leur capacité de réponse à l'ensemble des menaces qui peuvent toucher le SI d'INGEDEP. En ce sens, le DSI vous confie le projet d'audit et de renforcement de la sécurité du SI et vous demande :
a) d'établir un état des lieux de la sécurité du SI d'INGEDEP, en en soulignant les faiblesses mais aussi les atouts. (3 points)
b) d'identifier les menaces émergentes et les solutions à déployer en matière de virus. (2 points)

Question 2 (6 points)

INGEDEP a souhaité auditer sa chaîne de protection antivirale. Sur la base des conclusions de cet audit (annexe 2), de votre état des lieux (question 1a) et des solutions existantes pour répondre aux nouveaux risques (question 1b), vous présenterez :
a) l'architecture et l'organisation cible permettant de répondre aux problèmes recensés. (3 points)
b) la démarche projet préconisée permettant de mettre en œuvre cette nouvelle architecture cible. (3 points)

Question 3 (3 points)

L'analyse de la récente cyber-attaque démontre que le facteur humain est au centre de la sécurité et doit être pris en compte dans la gestion des risques du SI.
Vous présenterez un plan de mesures de responsabilisation et de sensibilisation permettant de mieux communiquer sur les bonnes pratiques informatiques et d'améliorer les réflexes des utilisateurs du SI face à des actions malveillantes.

Question 4 (3 points)

L'étude des risques sur les architectures techniques du SI d'INGEDEP a mis en évidence la complexité et la vulnérabilité de la plate-forme de sauvegarde ainsi que sa capacité à

satisfaire à l'évolution croissante des données de la collectivité. Les objectifs pour la direction des systèmes d'information sont la recherche d'une solution fonctionnelle plus efficace et garantissant la sécurité des données et la maîtrise des coûts d'exploitation.
Dans ce cadre, une migration totale ou partielle vers une solution de sauvegarde « cloud » est envisagée notamment pour les environnements et données de test.
Vous présenterez les avantages et inconvénients d'une telle solution dans le « cloud » ainsi que les enjeux juridiques, techniques et financiers.

Question 5 (3 points)

Le DSI doit présenter le projet aux élus et vous demande de préparer une note de synthèse reprenant l'ensemble des éléments permettant de valider les propositions de renforcement de son niveau de sécurité.

Liste des documents :

Document 1 : « Comment se prémunir de ces menaces ? » - ANSSI - *ssi.gouv.fr* - consulté le 5 avril 2019 - 1 page

Document 2 : « Les 10 chapitres du guide d'hygiène informatique de l'ANSSI » - Pierre-Alexandre Conte - *lagazettedescommunes.com* - 23 février 2017 - 2 pages

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

Document 4 : « Cybersécurité : attaques informatiques en cours et bonnes pratiques » (extrait) - *lyon-metropole.cci.fr* - consulté le 10 mai 2019 - 4 pages

Document 5 : « Les collectivités territoriales cibles des pirates informatiques » - Pierre-Alexandre Conte - *lenetexpert.fr* - 27 février 2017 - 3 pages

Document 6 : « Mathieu Vigneron, Atos : éviter les empilements de solutions de sécurité et de favoriser les solutions orchestrables » - Marc Jacob - *Global Security Mag* - octobre 2018 - 3 pages

Document 7 : « Comment appliquer le principe du Privacy by Design ? » (extrait) - Livre Blanc - *ageris-consulting.com* - 2 avril 2016 - 12 pages

Document 8 : « Méthode et outils à l'usage des équipes projet : Agilité & sécurité numériques » (extrait) - *ANSSI* - octobre 2018 - 30 pages

Document 9 : « Former et sensibiliser les agents à la sécurité informatique pour réduire les risques » - Pierre-Alexandre Conte - *lagazettedescommunes.com* - mis à jour le 23 février 2017 - 2 pages

Document 10 : « Prendre en compte et maîtriser le facteur humain dans la SSI » - Fiche SSI PRATIC N°9 - *assuris.fr* - janvier 2010 - 3 pages

Document 11 : « "Cloud" et souveraineté numérique : le débat fait rage » - Pierre-Alexandre Conte - *lagazettedescommunes.com* - 27 février 2017 - 2 pages

Document 12 : « Le PRA et le PCA revisités par le Cloud » - Olivier Bouzereau - *Solutions Numériques N°20* - 11 juin 2018 - 5 pages

Liste des annexes :

Annexe 1 : « Présentation générale des infrastructures » - *INGEDEP* - février 2019 - 3 pages

Annexe 2 : « Rapport d'audit de sécurité du Système d'Information (SI) » - *INGEDEP* - février 2019 - 2 pages

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.

ssi.gouv.fr - consulté le 5 avril 2019

COMMENT SE PRÉMUNIR DE CES MENACES ?

L'application des mesures d'hygiène préconisées par l'ANSSI, auxquelles le Centre de cyberdéfense a contribué en apportant son expérience opérationnelle, permettrait d'éviter plus de 80 % des attaques informatiques rencontrées.

La quasi-totalité des autres pourraient être évitées en exploitant de façon plus approfondie les guides et recommandations de l'agence.

Au quotidien, les principales lacunes de sécurité constatées par le Centre de cyberdéfense sont :

- des systèmes et des applications, dont les sites Web, qui ne sont pas à jour de leurs correctifs de sécurité
- une politique de gestion des mots de passe insuffisante (mots de passe par défaut ou trop simples et non renouvelés régulièrement…)
- une absence de séparation des usages entre utilisateur et administrateur des réseaux
- un laxisme manifeste dans la gestion des droits d'accès
- une absence de surveillance des systèmes d'information (analyse des journaux réseaux et de sécurité)
- un cloisonnement insuffisant des systèmes qui permet à une attaque de se propager au sein des réseaux
- une absence de restrictions d'accès aux périphériques (supports USB…)
- une ouverture excessive d'accès externes incontrôlés au système d'information (nomadisme, télétravail ou télé administration des systèmes)
- une sensibilisation et une maturité insuffisantes des utilisateurs et des dirigeants face à la menace dont ils ne perçoivent pas les risques.

DOSSIER : Sécurité informatique : comment se protéger ?
www.lagazettedescommunes.com

SÉCURITÉ INFORMATIQUE

Les 10 chapitres du guide d'hygiène informatique de l'Anssi

Pierre-Alexandre Conte | Dossiers d'actualité | France | Publié le 23/02/2017

L'Agence nationale de la sécurité des systèmes d'information a publié un Guide d'hygiène informatique, dont les mesures « sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire ».

01 – Sensibiliser et former.

L'Agence nationale de la sécurité des systèmes d'information (Anssi) recommande de sensibiliser les utilisateurs aux bonnes pratiques en termes de sécurité informatique, mais aussi de former les équipes opérationnelles pour éviter les erreurs générant des failles. Maîtriser les risques de l'infogérance en se posant les bonnes questions en amont est également important.

02 – Connaître le système d'information (SI).

Protéger efficacement les données sensibles nécessite de les identifier. Cela permet ensuite de localiser les postes à risque. Il faut aussi disposer d'un inventaire complet des comptes bénéficiant de droits étendus, veiller aux départs, aux arrivées et aux changements de fonctions. Enfin, les équipements qui s'y connectent doivent être maîtrisés.

03 – Authentifier et contrôler les accès.

L'Anssi incite à prêter attention au rôle de chaque personne, à attribuer les bons droits sur les ressources sensibles. Concernant l'accès au SI, les mots de passe doivent être correctement dimensionnés et, si besoin, stockés dans un endroit sécurisé. Lorsque cela est possible, l'authentification la plus forte doit être privilégiée.

04 – Sécuriser les postes.

Cette mesure implique de mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique, de configurer un pare-feu avec précaution, de chiffrer les données sensibles transmises par internet, de proscrire l'utilisation de supports amovibles tels que les clés USB et d'homogénéiser les politiques de sécurité.

05 – Sécuriser le réseau.

Outre le fait de protéger l'accès physique aux serveurs et aux locaux techniques, l'Anssi recommande de veiller à segmenter et à cloisonner le réseau pour éviter que toutes les machines soient liées entre elles. Utiliser des protocoles réseaux sécurisés, protéger la messagerie professionnelle, font partie des autres conseils.

06 – Sécuriser l'administration.

La navigation sur internet comporte de nombreux risques. Il convient donc d'interdire l'accès au web depuis les postes ou serveurs utilisés pour l'administration du SI. L'utilisation d'un réseau dédié et cloisonné est encouragée. Par ailleurs, il faut limiter au strict besoin opérationnel les droits d'administration.

07 – Gérer le nomadisme.

Il faut prendre des mesures de sécurisation physique, mais aussi chiffrer les données sensibles en cas de perte du matériel nomade. S'assurer de la sécurisation de la connexion de l'appareil au réseau du SI est aussi crucial. Plus globalement, adopter des politiques de sécurité dédiées aux terminaux mobiles apparaît indispensable.

08 – Maintenir le système d'information à jour.

Les failles contenues dans les logiciels sont particulièrement dangereuses. Mais elles sont progressivement corrigées. Aussi, il est important de s'équiper des versions les plus récentes des différents outils pour minimiser les risques. Anticiper la fin de leur maintenance est également essentiel.

09 – Superviser, auditer, réagir.

L'Anssi préconise, si possible, de désigner un RSSI, mais aussi de procéder régulièrement à des contrôles et audits de sécurité. Il convient également de mettre en place une politique de sauvegarde des composants critiques. En cas d'incident, disposer d'une procédure de gestion s'avère essentiel pour éviter de commettre des erreurs.

10 – Privilégier l'usage des produits et services qualifiés par l'Anssi.

L'agence propose une liste de produits et de prestataires qualifiés par ses soins. Elle encourage l'utilisation de ces derniers pour toute entité, car elle estime qu'il s'agit du seul gage d'une étude sérieuse et approfondie du fonctionnement technique de la solution et de son écosystème.

REFERENCES

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

DOSSIER : Sécurité informatique : comment se protéger ?
www.lagazettedescommunes.com

SÉCURITÉ INFORMATIQUE

Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance

Pierre-Alexandre Conte | Dossiers d'actualité | France | Publié le 23/02/2017

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.

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.

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. »

- Plusieurs milliers de sites Internet de communes mal sécurisés

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. »

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.

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.

REFERENCES

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

CHIFFRES CLES

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.

CCI LYON MÉTROPOLE
Saint-Etienne Roanne

Conseils sécurité

Cybersécurité : attaques informatiques en cours et bonnes pratiques

Se protéger contre la cybercriminalité est essentiel pour l'activité de votre entreprise. Quelques conseils pour vous prémunir contre les différentes cyber-attaques.

80 % des entreprises ayant subi un sinistre informatique majeur avec perte de données informatiques (mauvaise manipulation, virus, vol de données ou de matériel, fraude interne, déni de service...) **déposent le bilan dans les 2 années qui suivent.**

Vous trouverez ci-dessous quelques conseils sur les cyberattaques en cours et des conseils de bonnes pratiques.

Site Cybermalveillance.gouv.fr : le site national d'assistance et de prévention du risque numérique propose un **kit de sensibilisation à la cybermalveillance**, il traite des questions de sécurité du numérique, partage les bonnes pratiques dans les usages personnels, et vise à améliorer les usages dans le cadre professionnel.

Cyber-attaques en cours

Retrouvez ici les alertes de la Gendarmerie du Rhône et de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) sur les attaques informatiques constatées dernièrement.

Un nouveau site d'aide aux victimes

Le gouvernement a lancé Cybermalveillance.gouv.fr: le dispositif national d'assistance aux victimes d'actes de cybermalveillance. Ce service vise notamment à accueillir les victimes (particuliers, entreprises et collectivités territoriales) par le biais d'une plateforme numérique, et à les diriger vers les prestataires de proximité susceptibles de les assister techniquement. Un espace de sensibilisation informe également le public sur les risques des cyber-attaques. Les prestataires souhaitant proposer leurs services peuvent s'enregistrer sur la plate-forme.

Cyber-attaques de type ransomware ou rançongiciel

Qu'est-ce-qu'un "virus rançon" ?

Un ransomware (appelé également rançongiciel, crypto-virus ou virus rançon) est un logiciel malveillant pouvant entraîner soit le blocage d'un ordinateur, soit le chiffrement de données qu'il renferme, ou encore, la récupération des informations sensibles. Il ordonne ensuite le paiement d'une rançon (souvent en monnaie virtuelle, bitcoin) pour en restaurer l'accès.

ODIN : un virus ransomware , déclinaison de cryptohost

ODIN serait apparu pour la première fois le 29 septembre 2016. Il s'agit de la dernière déclinaison du ransomware LOCKY. Il utilise un système de cryptographie identique aux versions précédentes (Locky, Zepto, ...) mais chiffre les fichiers en leur ajoutant désormais une extension en « .odin ».

La clé ayant été modifiée, le déchiffreur « Autolocky », qui permettait depuis quelques temps de décrypter les fichiers en « .locky » est inefficace.

A l'instar de ses prédécesseurs, ce nouveau ransomware change l'image de fonds d'écran et laisse apparaître une fenêtre contenant les instructions de paiement, lequel sera effectué via le réseau TOR.

Alors que pour Locky, les cybercriminels exigeaient la somme de 360 euros (soit environ un bitcoin), la rançon désormais demandée s'élève à 2000 euros (toujours payable en bitcoins).

CRYPTOHOST : le virus qui verrouille vos données dans une archive RAR

Il se fait passer généralement pour le logiciel **P2P uTorrent** et se télécharge souvent sous le nom de uTorrent.exe pour tromper les utilisateurs. Un simple clic sur l'exécutable suffit pour l'activer.

CryptoHost, connu également sous le nom de Manamecrypt, ne chiffre pas directement vos fichiers. Il opère tout simplement en déplaçant vos fichiers dans une archive au format RAR protégée par un mot de passe. Il affichera par la suite trois messages différents sur votre bureau en vous précisant de régler la somme de 0.33 Bitcoins (environ 120 euros) pour récupérer vos données.

Récupérer les fichiers verrouillés par CryptoHost :

Une équipe de recherche composée de Michael Gillepsie, MalwareForMe, MalwareHunterTeam et enfin Bleeping Computer a découvert le moyen de récupérer ses données en déverrouillant l'archive sans payer cette fameuse rançon.

L'équipe révèle que le ransomware combine le numéro d'identification du processeur, le numéro de série de carte mère ainsi que celui du disque « C:\ » pour générer un algorithme de cryptographie. C'est cet algorithme qui est utilisé pour nommer l'archive RAR verrouillée. Par conséquent personne nepossède le même mot de passe... en fait il correspond tout simplement au nom de l'archive combiné à votre nom d'utilisateur.

Exemple : Si votre archive se nomme "9876543210FEDCBA01234" et que votre nom d'utilisateur c'est « Michel », votre mot de passe est le suivant : 9876543210FEDCBA01234Michel.

Avant de rentrer votre mot de passe, pensez à stopper le processus de CryptoHost en passant par votre gestionnaire de tâche (accessible en faisant CTRL + ALT + Suppr). Dans la liste des processus vous trouverez « *CryptoHost.exe* », il vous suffira de faire un clic-droit sur le processus et de choisir l'option « arrêter le processus ».

Il faudra bien évidemment procéder à la suppression de CryptoHost par la suite en supprimant le fichier suivant : *C:\Users\Nom d'utilisateur\AppData\Roaming folder\cryptohost.exe*.

Vous pouvez également supprimer la clé de registre correspondante en passant par votre éditeur de registre : *HKCU\Software\Microsoft\Windows\CurrentVersion\Run\software%AppData%\cryptohost.exe*

Source : Logithèque

JIGSAW : le ransomware qui lance un compte à rebours et menace de détruire vos fichiers

Il laisse une heure à sa victime pour payer la rançon, puis commence à détruire les fichiers de l'ordinateur en accélérant son rythme toutes les heures. Si aucun paiement n'est effectué dans un délai de 72 heures, tous les fichiers restants disparaissent.

Inactiver Jigsaw puis déchiffrer les fichiers à l'aide d'un utilitaire.

La première chose à faire, c'est d'ouvrir le gestionnaire de tâches de Windows et de terminer tous les processus appelés *firefox.exe* ou*drpbx.exe* qui ont été créés par le ransomware, indique Lawrence Abrams. Puis, il faut lancer l'utilitaire Windows MSConfig et supprimer l'entrée de démarrage pointant vers %UserProfile%\AppData\Roaming\Frfx\firefox.exe. Cela arrêtera le processus de destruction des fichiers et empêchera le malware de se relancer au redémarrage du système. Les utilisateurs pourront alors télécharger l'utilitaire "Jigsaw Decrypter" hébergé par BleepingComputer.com afin de déchiffrer leurs fichiers. Lorsque ce sera fait, il est hautement recommandé de télécharger un logiciel anti-malware à jour et de lancer un scan complet de son ordinateur pour désinstaller entièrement le ransomware.

Source : le Monde Informatique

PETYA

Petya est un ransomware qui chiffre l'ensemble du disque dur. Les cibles identifiées actuellement sont les entreprises : de faux emails de candidature menant vers des liens de téléchargement Dropbox sont utilisés.

Le G DATA Security Labs a détecté les premiers fichiers jeudi 24 mars en Allemagne.
La campagne actuellement en cours vise les entreprises. Dans un email au service des ressources humaines, il y a une référence à un CV se trouvant dans Dropbox. Le fichier stocké dans le partage Dropbox est un exécutable. Dès son exécution, l'ordinateur plante avec un écran bleu et redémarre. Mais avant cela, le MBR est manipulé afin que Petya prenne le contrôle sur le processus d'amorçage. Le système démarre à nouveau avec un message MS-Dos qui annonce une vérification CheckDisk. A défaut d'être vérifié, le système est chiffré et plus aucun accès n'est possible.
Le message est clair : le disque est chiffré et la victime doit payer une rançon en se connectant à une adresse disponible sur le réseau anonyme TOR. Sur la page concernée, il est affirmé que le disque dur est chiffré avec un algorithme fort. Après 7 jours, le prix de la rançon est doublé. Il n'y a pour le moment aucune certitude sur le fait que les données soient irrécupérables. Les experts du G DATA SecurityLabs travaillent à l'analyse de ce nouveau type de ransomware.
G DATA recommande aux entreprises et particuliers de redoubler de vigilance quant aux emails reçus. Dans les entreprises, le blocage des partages en ligne de type Dropbox est à étudier, ces systèmes permettant de passer à travers les filtrages des passerelles emails.
Nouveau : en utilisant un algorithme, il s'avère désormais possible de casser la clé de chiffrement interdisant l'accès aux données et de restaurer le Master Boot Record (MBR), la partition de démarrage qui permet à l'ordinateur d'initier le lancement de son système d'exploitation.

CTB LOKER
La nouvelle version du virus « CTB Locker » réussit à passer outre les firewalls et antivirus les plus sophistiqués,si ceux-ci sont mal configurés. « CTB Locker » se propage essentiellement **via des courriels d'apparence anodine**, personnalisés au maximum (notamment grâce à des informations recueillies par le biais des techniques dites de social engineering) en vue de ne pas éveiller les soupçons des utilisateurs ciblés. Un document, identifié comme étant une facture, une plainte de client, un bon de commande, …, comportant l'extension **« .cab »** (format de fichier Microsoft compressé) contient l'exécutable malveillant, lequel s'installe une fois le document ouvert puis crypte les données à l'insu de l'utilisateur. Peu de temps après, une fenêtre « pop -p » apparaît et informe le salarié de l'attaque dont il vient d'être victime et de la nécessité de payer une rançon avant l'échéance d'un compte à rebours affiché à l'écran pour obtenir un retour à la normale.
Payer se révèle souvent sans aucun effet car une fois la rançon réglée, le cybercriminel disparaît sans transmettre la clé de déchiffrement nécessaire au déblocage.

Autres ransomwares : LOCKY et CRYSIS
(Crysis venant du fait que ce dernier modifie les extensions des documents chiffrés en ".*Crysis*").
Il cible les entreprises et semble être installé par des attaques "bruteforce RDP". Si le groupe à l'origine de ce ransomware est le même que pour les autres attaques, **il y a probablement peu de chances de récupérer les documents chiffrés, même après paiement de la somme exigée.**
Comme dans les cas précédents, le fond d'écran est modifié avec les instructions de paiement adresse de contact dalailama2015@protonmail.ch par exemple.

Des règles de bon sens :
La première règle élémentaire de sécurité est la suivante : "On réfléchit puis on clique et non pas l'inverse".
Seule une vigilance de tous les instants peut éviter les désagréments causés par un ransomware.
La seconde règle de sécurité à appliquer par tous (*particuliers, administrations et entreprises privées*) est de réaliser des sauvegardes très régulières et d'en vérifier la viabilité. En cas de problème, cette action est la seule à permettre un retour à la normale (plus ou moins rapide) après avoir subi une

atteinte de ce type.

Comment se protéger contre le virus rançon ?

- **Sensibiliser régulièrement les salariés** et ce quel que soit le niveau de responsabilité exercé. Tout personnel connecté au réseau de l'entreprise est susceptible d'être rendu destinataire de mails piégés pouvant infecter au mieux son ordinateur et au pire l'intégralité du système d'information de l'entreprise.
- **Effectuer des sauvegardes régulières** de l'ensemble du système informatique et des données contenues. S'assurer régulièrement de leur viabilité.
- **Installer et mettre à jour régulièrement** antivirus et firewall.
- **Bloquer les extensions .cab** dans les applications messagerie
- **Effectuer une veille régulière** qui permettra d'anticiper et de s'adapter aux nouvelles menaces.

Que faire en cas de problème ?

- Prendre en photo tous les écrans (mail frauduleux et ses pièces-jointes) ou réaliser des copies d'écran et noter toutes les actions réalisées ainsi que les heures,
- Isoler les serveurs et lancer un scan antivirus,
- Identifier l'adresse IP émettrice du mail,
- Supprimer le profil utilisateur problématique sur les serveurs,
- Supprimer l'ensemble des fichiers cryptés,
- Restaurer l'ensemble des dossiers et fichiers depuis des sauvegardes ou des points de restauration système réalisés antérieurement à l'attaque,
- Communiquer immédiatement sur l'attaque auprès de tous les utilisateurs,
- Analyser en vue de comprendre les raisons pour lesquelles le mail n'a pas été filtré par les systèmes sécurité.

Procéder avec minutie au risque de perdre vos fichiers.

- **Dans tous les cas, déposer rapidement plainte** auprès du service de police ou de gendarmerie territorialement compétent en cas de problème avéré ou de simple tentative.

Première tentative réussie de ransomware sur MAC

Ke.Ranger ou **KeyRanger** est un malware transmis avec la version 2.9 du logiciel BitTorrent Transmission, est une bombe à retardement dont les premiers effets devraient se faire ressentir à compter du 07 mars 2016.

Et ces effets risquent d'être dévastateurs, si on ne met pas à jour immédiatement l'application en version 2.91, proposée depuis aujourd'hui par l'éditeur.

Trois jours après son installation, le malware va chiffrer les données de l'utilisateur puis lui réclamer une rançon s'il veut recouvrer ses données. C'est donc très grave pour ceux qui n'appliqueront pas la mise à jour de Transmission, ou qui n'effectueront pas les modalités pour supprimer le malware (lire : Transmission : gare au malware dans la version 2.9).

Une fois ce délai de grâce de 3 jours achevé, KeRanger contacte un serveur via une connexion anonymisée Tor. Il lance la procédure de chiffrement de certains dossiers et documents contenus dans le disque dur. **Une fois l'opération terminée, KeRanger réclame un paiement en Bitcoin d'une valeur équivalente à 400 $ pour déverrouiller les fichiers chiffrés.**

Les utilisateurs ayant installé la version 2.9 de Transmission vendredi sont donc susceptibles, dès aujourd'hui, d'être les victimes de Ke.Ranger.

Apple aurait réagi en supprimant le certificat du développeur permettant d'installer le malware.

Les ransomwares sont de plus en plus courants sur Windows, et jusqu'à présent le Mac était épargné. Ce n'est désormais plus le cas.

[…]

DOCUMENT 5

Les collectivités territoriales cibles des pirates informatiques

27 février 2017 - Par Pierre-Alexandre Conte

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.

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

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.

Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

Mathieu Vigneron, Atos : éviter les empilements de solutions de sécurité et favoriser les solutions orchestrables

Octobre 2018 par Marc Jacob

Pour sa nouvelle participation aux Assises de la Sécurité, Atos présentera sa gamme de solutions de cybersécurité avec en particulier ses offres de Gestion des identités et des accès, de protection des données, de communications mobiles sécurisées et ses services en sécurité. Mathieu Vigneron, Directeur commercial cybersécurité France chez Atos conseille entre autre d'éviter les empilements de solutions de sécurité et de favoriser les solutions orchestrables.

Global Security Mag : Qu'allez-vous présenter à l'occasion des Assises de la Sécurité ?

Mathieu Vigneron : Atos présentera une large gamme de solutions de cybersécurité, et mettra notamment en avant les points suivants : La Gestion des Identités et des Accès (IAM, E-SSO…) au sein des organisations lors du recours à des ressources et services externalisés et partagés, avec nos solutions Evidian. La protection des données et les produits de chiffrement Trustway. La mise en place d'une infrastructure sécurisée via des identités de confiance et la sécurité de l'Internet des Objets avec les solutions Horus. Les services en sécurité gérés depuis nos Security Operations Centers (SOCs), pour combattre les menaces – ainsi que la sécurité des applications et données d'entreprise dans le Cloud à l'heure de la mobilité. Les communications mobiles ultra-sécurisées avec notre smartphone Hoox.

GS Mag : Quel sera le thème de votre conférence cette année ?

Mathieu Vigneron : Nous organisons un atelier le jeudi 11 octobre à 10h au sujet de la mutualisation des solutions de gestion des accès et des identités entre les différentes filiales de l'entreprise Orange, grâce à notre solution Evidian IAM. Opérée centralement, la solution Evidian IAM facilite et harmonise les processus du Groupe, tout en respectant les spécificités fonctionnelles de chaque filiale.

Nous participerons également à l'atelier 'Transformez votre IT vers le Cloud en toute confiance' par McAfee, mercredi 10 octobre à 15h.

GS Mag : Quelles sont les principales menaces que vous avez pu identifier en 2018 ?

Mathieu Vigneron : Les principales menaces observées en 2018 sont directement liées aux grands chantiers digitaux engagés par nos clients. Les environnements techniques et métiers évoluent. Les risques aussi. Atos accompagne ses clients dans la gestion des menaces liées :
• Aux environnements hybrides (cloud public/privés – iaas, paas, saas) qui induisent la densification des flux est/ouest, les larges fédérations d'identités, la conteneurisation et les démarches devOps, à l'accroissement de la surface exposée via la multiplication des APIs et de leurs usages ;

• A l'avènement de l'intelligence artificielle et des algorithmes de machine-learning qui consomment et produisent de plus en plus de données avec plus ou moins de considérations quant à leur confidentialité et sensibilité ;

• A l'accélération de la convergence des environnements IT/OT qui expose brutalement des systèmes jusqu'à présent isolés et aux besoins de disponibilité et d'intégrité sans commune mesure avec la plupart des systèmes corporate.

GS Mag : Quid des besoins des entreprises ?

Mathieu Vigneron : La transformation digitale au cœur des préoccupations des entreprises. Il est nécessaire de comprendre les nouvelles menaces liées au changement de périmètre (Cloud, on-premises, IoT), de comprendre le niveau de maturité de l'entreprise en termes de sécurité pour définir comment faire évoluer la stratégie de l'entreprise.

▸ Les enjeux de mise en conformité (GDPR, LPM, NIS) sont toujours aussi nombreux. Les approches « théoriques » ne répondent pas au besoin. Nos clients recherchent des compromis acceptables entre business et sécurité/conformité.

▸ L'opération de la sécurité et les SOC sont au cœur de nombreuses réflexions chez nos clients. Beaucoup de demandes mais peu de projets qui voient effectivement le jour. Toutefois, le niveau de maturité évolue rapidement et nous observons une transition progressive des besoins de sécurité orientés « infrastructures » vers des besoins orienté « métiers » et construits sur des cas d'usage.

▸ S'outiller pour détecter des menaces toujours plus fines et discrètes dans des environnements très dynamiques et hétérogènes (cloud, mobilité, OT). L'approche « antivirus & signatures » ne suffit plus. Les besoins concernent la détection des comportements déviants, les capacité de sandoxing, les bases de réputation et les capacités de réaction et de quarantaine lorsqu'il y a un doute.

▸ Protéger les données (quelle que soit leur localisation). Comment décliner l'approche data-centric dans des contextes de migration vers le Cloud. Comment identifier les données sensibles (savoir-faire, propriété intellectuelles, données stratégiques, données personnelles, …). Evaluer les risques induits par le CloudAct/PatriotAct et construire une réponse adaptée (sans freiner la transformation digitale).

De quelle manière votre stratégie est-elle amenée à évoluer pour adresser ces enjeux ?

Mathieu Vigneron : Atos, en tant qu'ESN, accompagne ses clients dans leur transformation digitale et se positionne comme un partenaire de confiance. La division cybersécurité du groupe Atos a donc développé des solutions adaptées à ces nouveaux enjeux. Notre stratégie est aujourd'hui déclinée sur les piliers :

- Digitalisation du poste et de l'environnement de travail
- Hybridation des infrastructure dans le Cloud
- Intelligence Artificielle et Big Data

Atos fonde sa stratégie sur les compétences de ses propres collaborateurs et experts mais aussi en sélectionnant ses partenaires technologiques pour leur interopérabilité et pour leur capacité d'automatisation et d'orchestration (spécifiquement dans ces nouveaux contexte). Atos engage notamment ses efforts autour de :

- Nouvelles techniques d'authentification dans les environnements virtualisés
- Enclaves souveraines dans des environnements Cloud publics
- Outillage et méthode DevSecOPS

- SOC prescriptif
- Convergence des processus IT/OT et Ops/SSI

Nous accompagnons également les entreprises dans leur 'cybersecurity journey' autour des problématiques de sécurisation du cloud, du digital workplace, des identités de confiance, de la supervision des infrastructures, de sécurisation et de gouvernance des données, la sécurisation des milieux industriels.

GS Mag : Avec l'entrée en vigueur du RGPD, la « security & privacy by design » deviennent quasi incontournables. Quel sera votre positionnement en ce domaine ?

Mathieu Vigneron : Atos est acteur de la cybersécurité, en conseil, en intégration, en opérateur mais aussi en tant qu'éditeur de produits du domaine. La prise en compte de la cybersécurité est au cœur des processus mis en œuvre par les équipes cybersécurité depuis des années (et donc bien avant la mise en place du nouveau règlement européen).

La protection de nos systèmes et l'organisation de nos services/prestations est pilotée par les risques en termes d'atteinte à la confidentialité et à l'intégrité de nos données et de celles de nos clients.

Nous engageons aujourd'hui des efforts :

- de communication autour de ces systèmes de management pour expliquer les choix d'architectures qui ont été fait et qui sont fait quotidiennement avec nos clients.
- de protection des environnements/prestations DevOPS avec l'outillage sécurité adéquat (offre DevSecOPS) pour compléter les plateformes CICD existantes.
- de protection des architectures big-data et analytiques peu compatible, par nature, avec les principes du règlement européen.

Nous avons pour objectif accompagner et aider les entreprises depuis l'identification de leurs données personnelles avec le DPIA (data protection impact assessment) jusqu'à la mise en place des solutions adéquates pour les contrôler, les protéger et les superviser.

GS Mag : Quel est votre message aux RSSI ?

Mathieu Vigneron : J'en aurais deux :

1. Prenez de la hauteur. Construisez votre stratégie cybersécurité. Evitez les empilements ou les juxtapositions d'outils et favorisez les solutions orchestrables. Acceptez et accompagnez les transformations en profondeur des architectures et cherchez à rationnaliser votre modèle de défense en l'associant le plus possible aux cas d'usage de vos métiers. Le ROI n'en sera que plus facile à produire. Pour cela il faudra nécessairement identifier, qualifier et quantifier les risques, ainsi que se focaliser sur l'opération des technologies afin de pouvoir faire face aux menaces en perpétuelles évolutions.

2. Soyez au cœur, en tant qu'acteur, de la convergence des processus IT (opérations) et des processus sécurité. Œuvrez pour que la sécurité soit la plus intégrée possible au SI et accompagnez la transformation digitale (Cloud, IA, Digital workplace), de votre entreprise en proposant des solutions/réponses innovantes et orchestrées aux nouveaux enjeux. La stratégie sécurité de votre entreprise doit être alignée avec sa stratégie globale.

DOCUMENT 7

COMMENT APPLIQUER LE PRINCIPE DU PRIVACY BY DESIGN?

Livre Blanc - ageris-consulting.com - 2 avril 2016

TOUT D'ABORD, UN CONSTAT

Force est de constater que la prise en compte de la protection des données à caractère personnel (DCP) dès les phases amont d'un nouveau projet informatique n'est pas encore entrée dans les mœurs, ni des éditeurs de solutions, ni des donneurs d'ordre ou acheteurs.

Les contrôles de conformité de nature juridique réalisés par le CIL ou les audits de sécurité réalisés par le RSSI montrent que des efforts sont encore à consentir dans ce domaine.

Voici quelques exemples de sujets faiblement pris en compte voire totalement oubliés dans les démarches projets :

- L'application informatique déployée récemment ne prévoit pas de purge automatique des données des DCP dont le traitement n'est plus nécessaire.

- Les DCP restent stockées dans la base de données active pour une durée illimitée alors qu'elles devraient basculer dans une base de données intermédiaire, voire dans une base d'archivage en fonction de la finalité du traitement et du cadre légal applicable aux DCP concernées.

- L'application informatique ne prévoit pas de chiffrement des DCP permettant de limiter leur lisibilité aux seuls professionnels habilités à y accéder.

- Les DCP échangées en pièce jointe de courriel ne sont pas chiffrées ou protégées contre une lecture illicite notamment lors de l'usage de la messagerie sur internet.

- Les traces embarquées dans les applications informatiques sont difficilement exploitables (si elles existent) pour identifier l'origine d'une violation[1] sur les DCP.

- Les supports amovibles (exemple : clé USB) utilisés par les utilisateurs contiennent des DCP et ne sont pas protégés en cas de perte ou de vol.

[1] violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données [source : article 4 du projet de règlement européen]

- L'application informatique ne permet pas la mise en œuvre de solutions d'authentification forte (carte à puce par exemple) sans un développement complémentaire du fournisseur (si cela est possible) entrainant un surcoût non budgété.

- Les systèmes de surveillance et d'alarme ne sont pas programmés pour traiter les violations de DCP et les procédures de gestion des incidents ne prévoient pas la notification au responsable des traitements et/ou aux personnes concernées, des incidents sur les DCP les plus sensibles dans la limite de 72h00 après leur identification.

- Le cahier des charges ne contient pas de clauses spécifiques de sécurité des DCP imposant au fournisseur le respect de la politique de protection des DCP de l'organisme et des règles qui en découlent.

- Le fournisseur n'a pas suffisamment mis l'accent sur la sécurité des DCP dans les réponses au cahier des charges et n'a pas joint un plan d'assurance sécurité (PAS) à son dossier.

Les exemples sont malheureusement nombreux, et les failles de sécurité qui sont identifiées dans les démarches d'audit ou de contrôle sont parfois difficiles à colmater, voire impossibles à traiter.

L'ORIGINE DE CE CONSTAT

Il est difficile de pouvoir affirmer que l'origine de ce constat est unique. Cela dépend bien évidemment de l'organisme concerné, de sa maturité et des pratiques internes en matière de protection des données et des systèmes d'information.

Cependant, il est généralement admis qu'une absence de prise en compte ou une méconnaissance de ces sujets au plus haut niveau de l'organisme est souvent à l'origine d'une politique de protection des DCP insuffisamment adaptée aux enjeux, aux risques liés à l'usage des systèmes d'information et aux risques de nature juridique.

Il est à rappeler que la loi « informatique et libertés » (n° 78-17 du 6 janvier 1978 modifiée en 2004) précise en son article 34 : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. ».

Le responsable des traitements doit donc être informé de la nature des risques résiduels identifiés dans le cadre de contrôles ou mis en évidence lors d'un nouveau projet afin qu'il puisse décider des mesures de protection qui en découlent et assumer pleinement sa responsabilité de nature juridique.

De nombreuses questions restent encore trop souvent sans réponse positive :

- Le responsable des traitements est-il informé des risques numériques résiduels du nouveau projet informatique avant sa mise en production ?
- Le responsable des traitements a-t-il acté la prise en compte de mesures spécifiques de sécurité permettant de traiter les risques identifiés dans le cadre du nouveau projet avant sa mise en production ?
- Le responsable des traitements a-t-il homologué la sécurité informatique du nouveau projet et accepté les risques résiduels ?

COMMENT PROCEDER POUR AMELIORER LA SITUATION ?

Le prérequis à l'amélioration de la situation est la **mise en place d'une gouvernance** adaptée aux nouveaux enjeux réglementaires et aux nouveaux risques qui doit s'appuyer sur les éléments suivants :

- La création d'une **filière fonctionnelle « SSI[2] »** adaptée à l'organisme et prévoyant la désignation d'un RSSI (fonctionnellement rattaché à la Direction Générale) et la mise en place de référents SSI dans les directions métiers. Au niveau des maitrises d'œuvre (DSI, Moyens généraux), il convient également de désigner des responsables en charge de la mise en œuvre des politiques de sécurité ;

- La création d'une **filière fonctionnelle « Informatique et libertés »** s'appuyant sur le CIL et la mise en place de référents « Informatique et Libertés » dans les directions métiers (selon la taille de l'organisme bien évidement).

- La mise en place d'une **instance de décision**, placée sous la responsabilité du responsable des traitements et/ou dirigeant de l'organisme dont la mission sera de piloter, d'arbitrer et d'homologuer la sécurité des systèmes d'information. Il convient bien évidemment de rappeler aux dirigeants de l'organisme leurs rôles et responsabilités en matière de protection des DCP et des SI au travers de réunions de sensibilisation et d'ateliers d'échange afin qu'ils adhérent pleinement à la démarche.

Il est rappelé que l'ANSSI[3] impose la mise en place d'une gouvernance de la SSI au travers de différents référentiels et directives tels que la **PSSI-E** (Politique de Sécurité des Systèmes d'Information de l'Etat) ou le **RGS 2.0** (Référentiel Général de Sécurité).

Une fois les prérequis mis en œuvre, il convient ensuite que l**es équipes en charge de la mise en œuvre de nouveaux projets informatiques** (Chefs de projets Informatique (CPI) et Utilisateur (CPU)) soient formés et outillés pour intégrer la protection des DCP dès les phases amont des projets.

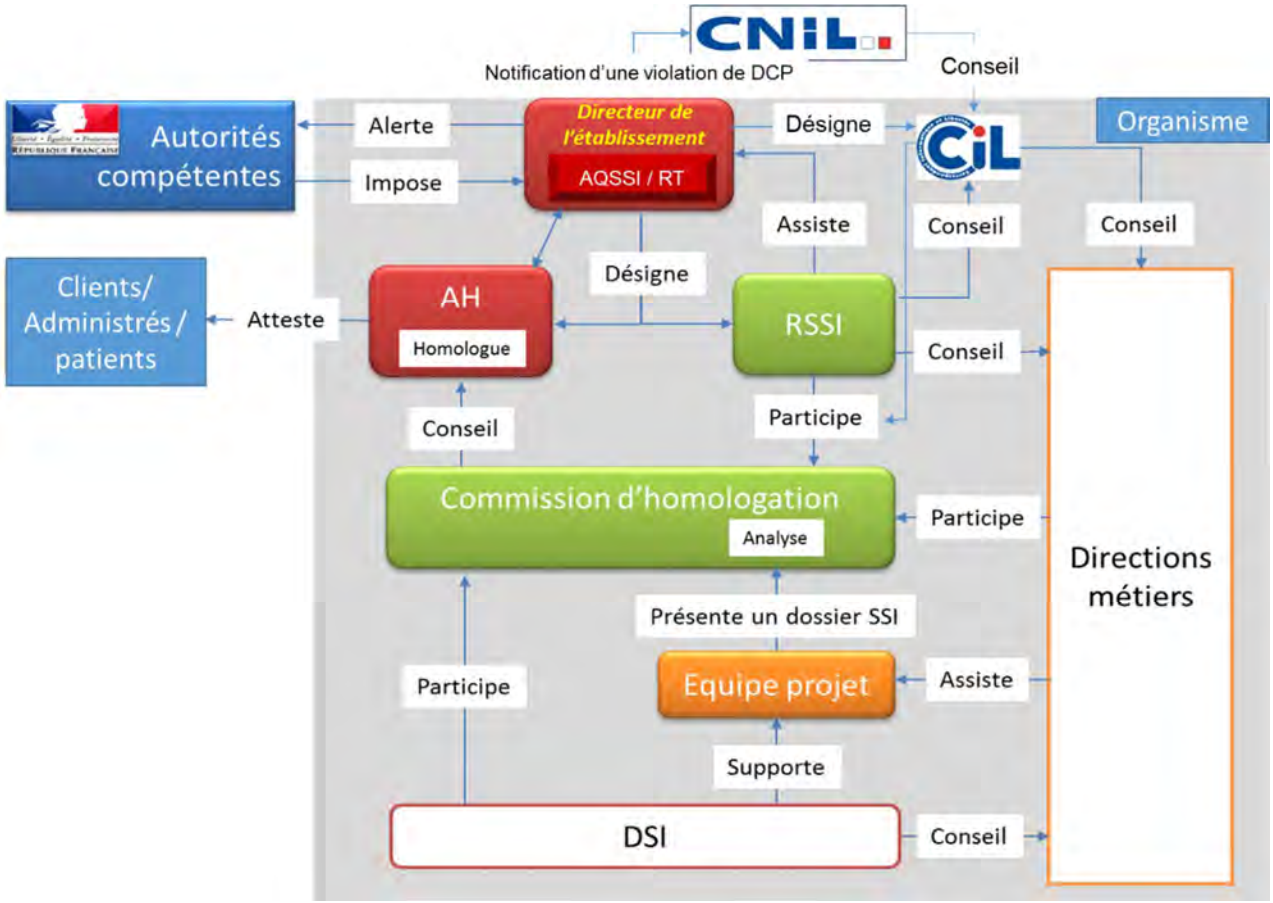
Le CIL et le RSSI sont des acteurs importants dans la mise en place de cette démarche et doivent réussir à faire adhérer pleinement à la démarche l'ensemble des acteurs impliqués (CPI, CPU, Chefs de Service, etc.).

L'équipe projet devra alors formaliser **un dossier de sécurité du nouveau projet** en vue d'une **homologation de la SSI** par le responsable des traitements et/ou le dirigeant de l'organisme en complément **d'un dossier d'évaluation d'impact sur la vie privée** si des données sensibles ou perçues comme sensibles sont traitées.

Le RSSI coordonne les actions relatives au dossier de sécurité, le CIL celles relatives à l'EIVP.

[2] SSI : Sécurité des Systèmes d'Information
[3] ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information (créée par le décret du 7 juillet 2009)

Le croquis ci-dessous donne un exemple de la gouvernance basée sur les recommandations de l'ANSSI que les organismes peuvent mettre en oeuvre :



AQSSI = Autorité Qualifiée en SSI
RT = Responsable des Traitements
AH : Autorité d'Homologation

QUE DOIT CONTENIR LE DOSSIER DE SECURITE PERMETTANT L'HOMOLOGATION DE LA SSI ?

Dans son « guide d'homologation de la SSI en 9 étapes[4] », l'ANSSI recommande la constitution d'un dossier SSI comprenant les documents suivants :

1. La stratégie d'homologation
2. L'analyse de risques
3. La politique de sécurité du système d'information (PSSI)
4. Le journal de bord de l'homologation
5. Les référentiels de sécurité
6. Le tableau de bord de l'application des règles d'hygiène informatique
7. La cartographie des systèmes d'information de l'organisme
8. Les schémas détaillés des architectures du système
9. Le document présentant les risques identifiés et les objectifs de sécurité

[4] Source : www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples - 20/03/2016

10. Les procédures d'exploitation du système
11. Les exigences de sécurité à destination des systèmes interconnectés
12. Les décisions d'homologation des systèmes interconnectés
13. Les certificats de sécurité des produits utilisés
14. Les attestations de qualification des produits ou prestataires
15. Les plans de tests et d'audits
16. Les rapports de tests et d'audits et les plans d'action associés
17. Le dossier des risques résiduels
18. Les éventuelles décisions d'homologation antérieures
19. Le tableau de bord des incidents et de leur résolution
20. Le journal des évolutions

La liste de documents à produire (20) parait exhaustive et lourde à appliquer mais elle permet au responsable des traitements de prendre pleinement connaissance de la situation, de pouvoir prendre les décisions qui s'imposent et d'assurer pleinement ses responsabilités de nature juridique.

Ne pas lui fournir les éléments recommandés par l'ANSSI, l'expose (le responsable des traitements) à une mauvaise prise de décision et expose l'équipe projet à des reproches quant à l'absence d'informations fournies pour la prise de décision notamment si une violation de DCP est constatée après la mise en production du projet.

2 APPROCHES, CELLE DE L'ANSSI ET CELLE DE LA CNIL : QUELLE DEMARCHE ADOPTER ?

L'ANSSI a fourni des recommandations concernant la démarche d'homologation à adopter notamment dans le RGS 2.0[5] et dans la PSSI-E[6] dont voici quelques extraits :

Extrait du RGS 2. 0 *: [Chapitre 1. Mise en conformité avec les exigences du « décret RGS »]*

« Afin de mettre leur système d'information en conformité avec le RGS, les autorités administratives doivent adopter une ***démarche en cinq étapes****, prévue par le décret n° 2010-112 du 2 février 2010 (décret RGS) :*

1. Réalisation d'une ***analyse des risques*** *(art. 3 al. 1) ;*

2. Définition des ***objectifs de sécurité*** *(art. 3 al. 2) ;*

3. Choix et mise en oeuvre des ***mesures appropriées*** *de protection et de défense du SI (art. 3 al. 3) ;*

4. ***Homologation*** *de sécurité du système d'information (art. 5) ;*

5. ***Suivi opérationnel*** *de la sécurité du SI.»*

Extrait de la PSSI-E *: [Deuxième Partie : objectifs et règles - Gestion des risques et homologation de sécurité]*

« INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information. Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'autorité qualifiée), le cas échéant après avis de la commission d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi. »

[5] RGS : Référentiel Général de Sécurité
[6] PSSI-E : Politique de Sécurité des Systèmes d'Information de l'Etat

La démarche imposée par l'ANSSI prévoit la réalisation d'une analyse des risques systématique et la définition des objectifs de sécurité comme point d'entrée permettant ensuite d'adapter les mesures de sécurité aux enjeux identifiés.

Par ailleurs, **la CNIL** a défini une méthodologie permettant d'évaluer l'impact sur la vie privée (EIVP)[7] qui prévoit :

1. De **décrire le (s) traitement(s)** considéré(s), les données à caractère personnel concernées et leur usage ;
2. **D'identifier les mesures existantes ou prévues** pour respecter les exigences légales et traiter les risques sur la vie privée des personnes concernées par le(s) traitement(s) ;
3. **D'apprécier les situations à risques** pour vérifier qu'ils sont convenablement traités au sein de l'organisme ;
4. De valider la manière dont il est prévu de respecter les principes de protection de la vie privée et de **valider les risques résiduels**.

Force est de constater que les 2 approches de l'ANSSI et de la CNIL sont proches et qu'elles introduisent les mêmes concepts :

1. Le périmètre doit être décrit pour bien **délimiter la cible de la démarche.**
2. Une **appréciation des risques** doit être réalisée par l'équipe projet. A noter que la CNIL s'appuie sur la méthode EBIOS de l'ANSSI pour identifier les risques sur les DCP.
3. La **décision finale revient au dirigeant / responsable des traitements** (homologation, acceptation de l'EIVP).

La matrice suivante décrit quelle démarche adopter en fonction de la nature du projet et des données traitées :

Type de projet	Démarche de l'ANSSI[8]	Démarche de la CNIL[9]
Nouveau projet informatique **avec** données à caractère personnel **non sensibles** au sens de la loi « informatique et libertés »	X	
Nouveau projet informatique **avec** données à caractère personnel **sensibles** au sens de la loi « informatique et libertés » ou perçues comme sensibles par la CNIL	X	X
Nouveau projet informatique **sans** donnée à caractère personnel	X	
Traitement déjà opérationnel **avec** données à caractère personnel **non sensibles** au sens de la loi « informatique et libertés »	X	
Traitement déjà opérationnel **avec** données à caractère personnel **sensibles** au sens de la loi « informatique et libertés » ou perçues comme sensibles par la CNIL	X	X
Traitement déjà opérationnel **sans** donnée à caractère personnel	X	

[7] Le livre Blanc d'AGERIS Priv@cy décrit la démarche EIVP : www.slideshare.net/ThierryRAMARD/ageris-privcy-livre-blanc-sur-lvaluation-dimpact-sur-la-vie-prive-eivp

[8] Guide d'homologation en 9 étapes

[9] Guide d'évaluation d'impact sur la vie privée (EIVP)

METHODOLOGIE A APPLIQUER LORSQU'IL EST PREVU DE TRAITER DES DCP SENSIBLES OU PERÇUES COMME SENSIBLES DANS LE CADRE DU NOUVEAU PROJET

La démarche méthodologique, basée sur les recommandations des autorités compétentes (CNIL et ANSSI) pourrait être la suivante :

La démarche	Les actions	Outillages ou référentiels disponibles
Décrire le périmètre du projet	1. Identifier le contexte et les contraintes éventuelles du projet	Guide d'homologation en 9 étapes
	2. Décrire le(s) traitement(s) considéré(s), les données à caractère personnel concernées et leur usage	Guide EIVP de la CNIL
Identifier les mesures existantes ou prévues	3. Décrire les mesures existantes ou prévues pour respecter les exigences légales	Guide EIVP de la CNIL
	4. Décrire les mesures pour traiter les risques sur la vie privée des personnes concernées par le(s) traitement(s)	Guide EIVP de la CNIL Guide d'hygiène informatique de l'ANSSI Norme ISO 27002
Identifier les besoins de sécurité du SI	5. Faire une estimation rapide des besoins SSI du projet / Classification des informations et des actifs en support	Guide d'homologation en 9 étapes
Analyser les risques sur les DCP	6. Identifier les sources de risques	Guide EIVP de la CNIL
	7. Analyser l'impact des évènements redoutés pour les personnes concernées	Guide EIVP de la CNIL
	8. Analyser la vraisemblance de scénarios de menaces	Guide EIVP de la CNIL
	9. Dresser la cartographie des risques résiduels	
Valider l'EIVP & homologuer la SSI	10. Mettre en évidence les non-conformités de nature juridique	Guide EIVP de la CNIL
	11. Décider de la stratégie de traitement des risques résiduels	Guide EIVP de la CNIL
	12. Définir le plan d'actions de réduction des risques	Guide EIVP de la CNIL Guide d'hygiène informatique de l'ANSSI
	13. Faire auditer la SSI du projet par un tiers indépendant	Guide d'homologation en 9 étapes
	14. Formaliser le dossier de sécurité du projet	Guide d'homologation en 9 étapes
	15. Homologuer la SSI du projet	Guide d'homologation en 9 étapes
	16. Formaliser une attestation formelle d'homologation et de validation de l'EIVP	Guide EIVP de la CNIL Guide d'homologation en 9 étapes

Ces étapes peuvent bien évidemment être plus ou moins importantes et complexes en fonction de la nature du projet.

QU'ELLE EST LA DUREE DE VALIDITE D'UNE HOMOLOGATION DE LA SSI[10] ?

L'homologation de la SSI d'un projet doit être décidée pour une durée maximale.

Cette durée doit prendre en compte l'exposition du système d'information aux nouvelles menaces, ainsi que les enjeux de sécurité du système, c'est-à-dire le degré de criticité des informations et des processus du système.

Pour un système bien maîtrisé, avec peu de risques résiduels et ne présentant pas de difficultés particulières, il est recommandé de prononcer une **homologation d'une durée maximale de cinq (5) ans, avec revue annuelle**.

Cette durée maximale doit être réduite **à trois (3) ans** pour un système avec de nombreux risques résiduels ou à **un (1) an** pour un système présentant de nombreux risques résiduels.

L'homologation peut être retirée dans le cas où les circonstances l'imposent. Ainsi, l'ANSSI identifie, dans son guide d'homologation en 9 étapes, les évènements suivants pouvant impliquer un réexamen du dossier, pouvant conduire à une nouvelle décision d'homologation ou pouvant conduire à un retrait de la décision :

- Raccordement d'un nouveau site sur le système d'information ;
- Ajout d'une fonctionnalité majeure ;
- Succession de modifications mineures ;
- Réduction de l'effectif affecté à une tâche impactant la sécurité ;
- Changement d'un ou de plusieurs prestataires ;
- Prise de fonction d'une nouvelle autorité d'homologation ;
- Non-respect d'au moins une des conditions de l'homologation ;
- Changement du niveau de sensibilité des informations traitées et, plus généralement, du niveau du risque ;
- Evolution du statut de l'homologation des systèmes interconnectés ;
- Publication d'incidents de nature à remettre en cause les garanties recueillies dans le dossier de sécurité ;
- Décision de l'autorité d'homologation.

À ce titre, il est recommandé que l'instance de décision (la commission d'homologation) soit réunie annuellement par l'autorité d'homologation (AH), afin de procéder à une revue du respect des conditions de l'homologation.

[10] Source : Source : www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples - 20/03/2016

QUELLES SONT LES MESURES DE SECURITE QUI PEUVENT ETRE MISE EN ŒUVRE DANS LE CADRE D'UN NOUVEAU PROJET ?

La CNIL a diffusé en 2012 un guide des «mesures pour traiter les risques sur les libertés et la vie privée»[11].
Ce guide identifie **34 mesures dans 5 domaines** dont voici la liste :

Domaines	Mesures proposées par la CNIL
01 -Minimiser les Données à Caractère Personnel	01-Agir sur les éléments à protéger 02 -Gérer les durées de conservation des Données à Caractère Personnel 03 -Informer les personnes concernées 04 -Obtenir le consentement des personnes concernées 05-Permettre l'exercice du droit d'opposition 06-Permettre l'exercice du droit d'accès direct 07-Permettre l'exercice du droit de rectification 08-Cloisonner les Données à Caractère Personnel 09-Chiffrer les Données à Caractère Personnel 10-Anonymiser les Données à Caractère Personnel
2-Agir sur les impacts	11-Sauvegarder les Données à Caractère Personnel 12-Protéger les archives des Données à Caractère Personnel 13-Contrôler l'intégrité des Données à Caractère Personnel 14-Tracer l'activité sur le système informatique 15-Gérer les violations sur les Données à Caractère Personnel
3-Agir sur les sources de risque	16-S'éloigner des sources de risques 17-Marquer les documents contenant des Données à Caractère Personnel 18-Gérer les personnes internes qui ont un accès légitime 19-Contrôler l'accès logique des personnes 20-Gérer les tiers qui ont un accès légitime aux Données à Caractère Personnel 21-Lutter contre les codes malveillants 22-Contrôler l'accès physique des personnes 23-Se protéger contre les sources de risques non humaines
4-Agir sur les supports	24-Réduire les vulnérabilités des logiciels 25-Réduire les vulnérabilités des matériels 26-Réduire les vulnérabilités des canaux informatiques 27-Réduire les vulnérabilités des personnes 28-Réduire les vulnérabilités des documents papier 29-Réduire les vulnérabilités des canaux papier
5-Actions transverses	30-Gérer l'organisation de protection de la vie privée 31-Gérer les risques sur la vie privée 32-Gérer la politique de protection de la vie privée 33-Intégrer la protection de la vie privée dans les projets 34 -Superviser la protection de la vie privée

[11] Source : www.cnil.fr/sites/default/files/typo/document/CNIL-Guide_securite_avance_Mesures.pdf - 20/03/2016

Il ne s'agit bien évidemment pas d'appliquer systématiquement l'ensemble de ces mesures ; elles doivent être sélectionnées et dimensionnées en fonction des risques identifiés sur la vie privée des personnes concernées.

L'ensemble de ces mesures fait l'objet d'explications et d'aides à la mise en œuvre ce qui représente aux alentours de 400 préconisations formulées par la CNIL. Ce guide permet donc de prendre en compte la plupart des cas spécifiques relatifs aux traitements de DCP et permet d'élaborer un plan d'action précis pour réduire les risques à un niveau acceptable pour les personnes concernées et pour l'organisme en charge de la mise en œuvre des traitements.

D'autres référentiels bien connus des RSSI peuvent également servir de documents de travail tels que les bonnes pratiques énoncées dans la norme **ISO 27002 : 2013** ou les **40 règles d'hygiène informatique** proposées par l'ANSSI.

Enfin, dans le cas où l'organisme dispose d'une **PSSI** validée par la Direction Générale, les règles fonctionnelles et/ou techniques y figurant doivent bien évidemment servir de base de travail pour les équipes projets. Dans tous les cas contraires, **il est recommandé de formaliser une politique interne de protection des DCP et une politique de sécurité des SI (PSSI)** qui servira de référentiel interne pour tout nouveau projet.

LES MESURES DE NATURE JURIDIQUE QUI DOIVENT IMPERATIVEMENT ETRE APPLIQUEES

Des principes et droits fondamentaux «non négociables», qui sont fixés par la loi, doivent être respectés et ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus[12].

Ainsi les 11 principes et droits fondamentaux suivants doivent être systématiquement appliqués dans tout nouveau projet informatique :

1. **Finalité** : les DCP doivent être collectées pour des finalités déterminées, explicites et légitimes conformément à l'article 6 de la [Loi-I&L] et de la [Directive-95-46].

2. **Minimisation** : Les DCP doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs conformément à l'article 6 de la [Loi-I&L] et de la [Directive-95-46]).

3. **Qualité** : les DCP doivent être exactes, complètes et, si nécessaire, mises à jour conformément à l'article 6 de la [Loi-I&L] et de la [Directive-95-46]). L'exigence de qualité porte également sur le lien entre les données qui identifient les personnes et les données qui les concernent.
4. **Durées de conservation** : Les DCP doivent être conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées conformément à l'article 6 de la [Loi-I&L] et de la [Directive-95-46], à défaut d'une autre obligation légale imposant une conservation plus longue.

5. **Information** : Le respect du droit à l'information des personnes concernées doit être appliqué conformément à l'article 32 de la [Loi-I&L] et aux articles 10 et 11 de la [Directive-95-46]).

6. **Consentement** : L'obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement doit être respecté conformément à l'article 7 de la [Loi-I&L].

[12] Source : www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf

7. **Droit d'opposition** : Le droit d'opposition des personnes concernées doit être respecté conformément à l'article 38 de la [Loi-I&L] et article 14 de la [Directive-95-46].

8. **Droit d'accès** : Le droit des personnes concernées d'accéder à leurs données doit être respecté conformément à l'article 39 de la [Loi-I&L] et article 12 de la [Directive-95-46].

9. **Droit de rectification** : Le droit des personnes concernées de corriger leurs données et de les effacer doit être appliqué ; La personne concernée peut demander que les «données inexactes, incomplètes, équivoques, périmées» ou dont «la collecte, l'utilisation, la communication ou la conservation est interdite» soient supprimées conformément à l'article 40 de la [Loi-I&L] et article 12 de la [Directive-95-46]).

10. **Transferts** : Les obligations en matière de transfert de données en dehors de l'Union européenne doivent être respectées en conformité avec les articles 68 et 69 de la [Loi-I&L] et les articles 25 et 26 de la [Directive-95-46]).

11. **Formalités** : définition et accomplissement des formalités préalables applicables au traitement.

Il convient donc que le cahier des charges technique formalisé dans le cadre du nouveau projet impose des directives aux développeurs internes ou aux sous-traitants / partenaires externes pour que les applications informatiques intègrent, intrinsèquement et dès que cela est possible, des mécanismes automatiques pour traiter les 11 fondamentaux évoqués.

Toute impossibilité de mise en œuvre doit être justifiée et des solutions de contournement doivent être proposées par le tiers ou le développeur pour traiter les obligations légales.

RECOMMANDATIONS POUR METTRE EN ŒUVRE LA DEMARCHE « PRIVACY BY DESIGN »

La mise en place d'une démarche de prise en compte la protection des DCP dans les nouveaux projets implique les éléments suivants :

1. **La Direction générale** de l'organisme doit être impliquée dans le processus notamment pour l'imposer à tous les acteurs et pour prendre les décisions qui s'imposent (homologation ou non de la SSI, validation ou non de l'EIVP, choix des mesures de protection, ….). Des actions de sensibilisation à la démarche sont nécessaires pour que la bonne compréhension des rôles et des responsabilités des uns et des autres.

2. **La démarche projet** de l'organisme doit être adaptée pour intégrer la prise en compte du processus à chacune des étapes du projet. A noter que l'ANSSI a diffusé un guide d'intégration de la SSI dans les projets[13] qui décrit les livrables à prévoir par le chef de projet à chaque étape de celui-ci.

3. **Les chefs de service en charge de la mise en œuvre d'un nouveau traitement** doivent être impliqués dans la démarche afin de participer à l'évaluation d'impact sur la vie privée au même titre que les chefs de projet (CPI et CPU) qui auront un rôle plus spécifique dans la formalisation du dossier de sécurité du projet.

[13] www.ssi.gouv.fr/guide/40-gissip-guide-dintegration-de-la-securite-des-systemes-dinformation-dans-les-projets

4. **Les RSSI et les CIL** sont incontournables dans la démarche et constituent un binôme « socle » de la démarche. Dans un premier temps, ils accompagnent au changement les équipes concernées, ensuite ils contribuent à donner un avis au dirigeant de l'organisme sur la décision à prendre concernant l'homologation de la SSI et la validation de l'EIVP.

5. **Les sous-traitants ou les partenaires** doivent également être impliqués dans le processus lors de la mise en œuvre des mesures de sécurité et dans l'élaboration du plan d'assurance SSI.

6. **Une phase pilote** doit probablement être mise en œuvre avant d'envisager une généralisation du processus pour tous les nouveaux traitements de DCP et tous les nouveaux projets informatiques notamment si la maturité de l'organisme sur le sujet est faible.

7. **Des actions de formation et de sensibilisation** sont indispensables au démarrage de la démarche afin que chacun s'approprie le processus et son rôle dans la démarche.

8. **Un outillage adapté peut s'avérer nécessaire** pour faciliter la réalisation des différentes étapes notamment pour apprécier les risques et définir les plans d'action.

9. **Une aide externe** pour la mise en œuvre de la démarche pourrait s'avérer utile pour éviter les erreurs dans la réalisation des étapes et capitaliser sur des expériences acquises.

10. **La gouvernance SSI et « Informatique et Libertés »** et la mise en place des **filières fonctionnelles** est le prérequis indispensable à la réussite de la démarche. Le RSSI et le CIL doivent agir pour que l'organisation, les rôles et les responsabilités soient établis avant de mettre en œuvre le processus complet.

[...]

Méthode et outils à l'usage des équipes projet

Agilité & sécurité numériques

ANSSI - Octobre 2018

SOMMAIRE

AGILITÉ & SÉCURITÉ NUMÉRIQUES

Méthode et outils à l'usage des équipes projet

PRÉFACE

La maîtrise pleine et entière du numérique – de ses programmes, de ses outils, de ses méthodes et même de ses codes – est aujourd'hui une dimension essentielle de la sécurité et de la souveraineté. L'État, au même titre que les entreprises, ne peut se contenter d'être le consommateur passif de solutions développées par d'autres, pas plus qu'il ne peut se satisfaire d'anciennes méthodes et de protocoles figés.

C'est pourquoi l'agilité et la sécurité doivent désormais être intégrées, au plus tôt et en permanence, dans la conduite de projets et ainsi nourrir efficacement la prévention des risques numériques et la détection des cyberattaques. Si l'idée fait son chemin, sa mise en œuvre tarde encore à se généraliser.

C'est donc avec beaucoup d'enthousiasme que l'ANSSI et la DINSIC ont décidé de conjuguer leurs expertises respectives en matière de sécurité numérique et de gestion de projet agile pour proposer une méthodologie commune résolument pratique et concrète.

Pour la DINSIC, la sécurité des services dématérialisés qu'elle développe est une valeur cardinale qui conditionne l'efficacité de tout projet, la sûreté de l'État et, bien souvent, la protection de la vie privée des citoyens. Pour l'ANSSI, l'agilité est un impératif face à un état de la menace en mouvement permanent.

La méthode que propose ce document repose donc avant tout sur l'expérience de celles et ceux qui, conscients de la valeur de cette alliance, la mettent en œuvre et la font évoluer à chaque nouveau projet. Pour preuve, le cœur de la démarche repose sur l'organisation d'ateliers d'appréciation des risques et prépare efficacement à l'homologation des services numériques et applications.

Nous tenons à remercier nos équipes qui ont su partager et enrichir leurs convictions et priorités respectives ainsi que tous ceux qui, par leur participation à l'appel à commentaires, ont fait de ce guide un outil qui saura faire écho à la réalité des équipes projet !

Guillaume Poupard
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information (ANSSI)

Henri Verdier
Directeur interministériel du numérique et du système
d'information et de communication de l'État (DINSIC)

1 À QUI S'ADRESSE CE GUIDE ?

À QUI S'ADRESSE CE GUIDE ?

Intitulé *« Agilité & sécurité numériques – Méthode et outils à l'usage des équipes projet »*, ce guide explique de manière pratique et concrète aux équipes d'entités publiques et privées comment conduire un développement numérique dans le cadre d'une *équipe agile* tout en considérant le volet *sécurité*.

De l'analyse au traitement des risques numériques, des fiches mémo, exemples et ressources documentaires **vous accompagnent pas à pas dans le développement sécurisé de vos *services* ou *produits*.**

Plus précisément, sont concernées par ce document les équipes dont :

- le principal objectif est de livrer rapidement et fréquemment un produit ou un service à ses usagers, pour résoudre un problème auquel ceux-ci sont confrontés ;
- les membres sont dotés de compétences diverses – techniques ou non – et travaillent ensemble au quotidien ;
- les membres sont suffisamment autonomes pour décider ensemble de l'organisation de leur propre travail ;
- l'attention est prioritairement tournée vers la qualité de ce qu'elles produisent et qui s'outillent en conséquence dans un souci permanent d'amélioration.

Généralement, ces caractéristiques – sans être individuellement essentielles à « l'agilité » – s'observent dans des équipes plutôt réduites de cinq à dix personnes et s'accompagnent de pratiques telles que le management visuel (*task board*, etc.), l'utilisation systématique de tests automatisés, le déploiement continu, les outils DevOps et le cadencement du travail en itérations. Nous désignons l'ensemble des intervenants d'une telle équipe par le terme *équipe produit*.

La sécurité numérique concerne toute organisation et tous types de projets. La méthode d'identification et de traitement des risques décrite dans ce guide permet de mettre en évidence quels sont, parmi ces risques numériques, les plus conséquents dans le contexte d'usage du service ou du produit. La nature des risques à considérer est variée.

Citons, par exemple, les actions de sabotage par déni de service distribué, le vol de données économiques ou à caractère personnel, la fraude ou le détournement d'usage à des fins lucratives, l'usurpation d'identité ou encore les actions de déstabilisation et d'atteinte à la réputation.

NOTES

1
À QUI S'ADRESSE CE GUIDE ?
AGILITÉ & SÉCURITÉ NUMÉRIQUES

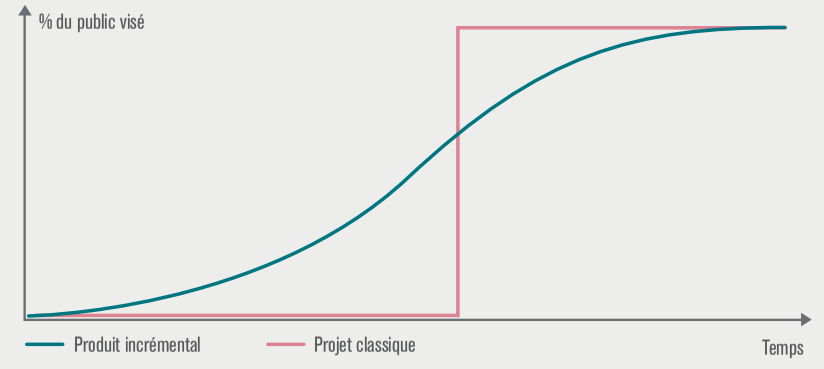
2/ LA PRISE EN COMPTE INCRÉMENTALE DU RISQUE

LA PRISE EN COMPTE INCRÉMENTALE DU RISQUE : LA CLÉ DE LA COMPATIBILITÉ AGILE

Dans une démarche sécuritaire classique, l'équipe définit les besoins de sécurité et les façons d'y répondre dès la phase de conception d'un **projet**, les mesures de sécurité étant très souvent définies et mises en œuvre pour le périmètre final et son cas d'usage à la cible. Dans une démarche agile, l'équipe cherche à livrer très tôt de la valeur à un public donné avec un **produit** incomplet, tout en cherchant à susciter l'adhésion d'autres publics en étoffant ce produit.

Voici, illustrées, deux conceptions opposées : ce que peut être la courbe de diffusion d'un produit, comparée à celle résultant de la livraison d'un projet.

Diffusion d'un produit vs livraison d'un projet

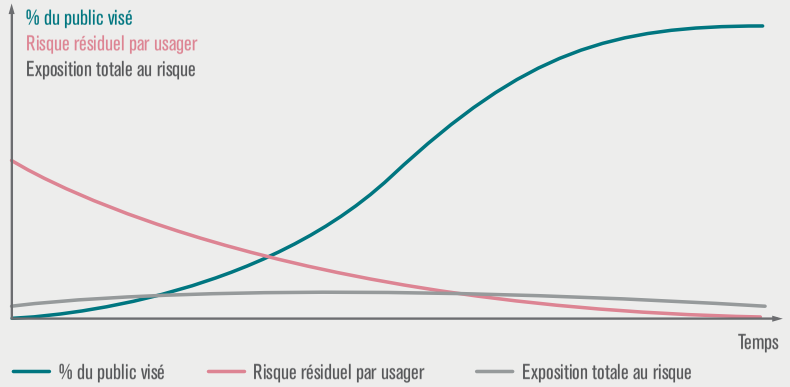


Pour une équipe dont l'objectif est de livrer rapidement de la valeur à ses utilisateurs, une évaluation pertinente du risque est donc obtenue en considérant simultanément le nombre d'usagers et le risque encouru par chacun, pour déterminer une exposition globale au risque.

Ainsi, la prise en compte des enjeux de sécurité par une équipe agile se veut continue (tout au long de la construction et de l'amélioration du service) et pragmatique puisqu'elle priorise les efforts en fonction du risque réel et assume l'existence de risques résiduels. **Ce principe de management de la sécurité numérique par les risques est celui qui guide la démarche proposée.**

La figure ci-dessous superpose à la courbe de diffusion une courbe hypothétique représentant le risque résiduel auquel un seul usager serait exposé. Initialement, le risque par usager est substantiel, mais avec une poignée d'utilisateurs, il reste globalement acceptable. En revanche, lorsque le produit devient un succès, l'équipe doit alors renforcer le traitement des risques résiduels.

Exposition au risque résiduel d'un produit



L'important est donc de s'assurer d'arriver au point d'inflexion en ayant couvert les risques numériques les plus importants, la recherche de l'exhaustivité n'étant pas forcément prioritaire, sous peine d'allouer des ressources conséquentes pour un résultat mitigé alors que ces dernières auraient pu être investies dans une meilleure compréhension du besoin.

NOTES

2/
LA PRISE EN COMPTE INCRÉMENTALE DU RISQUE
AGILITÉ & SÉCURITÉ NUMÉRIQUES

3/ L'ATELIER D'ANALYSE DE RISQUE

L'ATELIER D'ANALYSE DE RISQUE : LE CŒUR DE LA DÉMARCHE

Nos recommandations concrètes envers les équipes agiles peuvent se résumer ainsi : **l'équipe se réunit, à intervalles réguliers, pour discuter des risques numériques qui peuvent impacter les usagers de son service ou produit et décider de la meilleure manière de traiter ces risques.**

Un atelier type d'analyse de risque se déroule dans les conditions suivantes :

- présence de toute l'équipe et seulement de l'équipe ;
- durée fixe et limitée (une à trois heures), mieux vaut privilégier la programmation de plusieurs ateliers.

Le support d'animation de l'atelier peut reposer sur l'utilisation d'un *paper board* ou de Post-it pour accompagner la discussion et animer les éléments d'analyse de risque qui auront été consignés sur des feuillets.

/ QUAND FAUT-IL TENIR CES ATELIERS ?

L'adage est bien connu : *« Le meilleur moment pour planter un arbre, c'était il y a 20 ans ; le deuxième meilleur moment, c'est maintenant. »* Il n'est jamais trop tard pour parler de sécurité numérique et évaluer les risques inhérents à la conduite d'un projet donné, idéalement **avant même le début des travaux de réalisation, voire d'investigation**. Néanmoins, le fait que l'équipe ait déjà réalisé un ou plusieurs incréments de fonctionnalité, voire que son produit soit déjà accessible à de premiers usagers, ne saurait constituer une raison valable de ne pas se livrer à l'exercice.

/ COMMENT ANIMER L'ATELIER ?

Les conditions du succès d'un atelier d'analyse de risque sont à rapprocher de celles d'autres « rituels » agiles, comme par exemple la rétrospective. **Véritable facilitateur, l'animateur de ces ateliers assume un rôle particulièrement important dont voici quelques-unes des principales responsabilités :**

- s'assurer que la prise de parole est répartie de façon équilibrée entre les différents participants à l'atelier ;
- veiller à ce que le groupe ne dévie pas du sujet à traiter ;
- maintenir un climat bienveillant ;
- surveiller l'horloge… Un bon atelier ne déborde pas (trop) du temps imparti.

Une animation efficace suppose également de bien maîtriser le canevas d'analyse de risque ; celui-ci est présenté schématiquement plus loin (section *« L'appréciation des risques : les bases à connaître et à transmettre »* page 20) et de façon plus détaillée et analytique en fiche mémo page 42.

/ FAUT-IL SE FAIRE ACCOMPAGNER ?

La présence d'un expert en sécurité numérique n'est pas indispensable à la réussite de la démarche. Quelles que soient les conclusions de l'analyse de risque, c'est à l'équipe dans son ensemble qu'il incombera de mettre en œuvre les actions qui s'en dégagent et c'est notamment en cela que s'illustre l'agilité d'une équipe.

Un atelier de travail n'est pas une réunion. L'efficacité d'un atelier est conditionnée par une prise de parole et d'initiative équilibrée entre participants. Elle risque d'être diminuée par la présence d'observateurs ou de personnes non impliquées (ou très indirectement) dans la réalisation du produit.

Le niveau de maturité et de compétence au sein de l'équipe en matière de sécurité numérique pèsera lui aussi de façon déterminante sur les résultats de la démarche. Si l'équipe ne maîtrise pas suffisamment ces compétences au démarrage, il lui faudra donc les acquérir. La présence d'un expert en sécurité numérique, dans une posture de service et d'accompagnement, peut donc être un facteur de réussite. Il ou elle pourra jouer un rôle d'animation ou de facilitation, mais également faire bénéficier de son expertise lorsque c'est opportun.

3/ L'ATELIER D'ANALYSE DE RISQUE
AGILITÉ & SÉCURITÉ NUMÉRIQUES

4 LE PREMIER ATELIER

LE PREMIER ATELIER

En amont du premier atelier voire en début de séance, il est important de définir le périmètre de l'analyse.

- Y est inclus : ce qui engage la responsabilité de l'équipe et de sa hiérarchie.
- En est exclu : ce qui relève éventuellement d'autres acteurs.

Pour lancer ce premier atelier, vous pouvez proposer le cadrage suivant :

- *Un mois après le lancement du produit, vous découvrez avec horreur un article dans la presse nationale qui fait état d'une énorme faille de sécurité exploitée avec succès. Quels scénarios de menaces possibles vous viennent à l'esprit ?*

Cet exercice permettra de concentrer l'attention des participants sur les enjeux et besoins de sécurité les plus importants tout en amorçant la discussion. Lorsque celle-ci cesse de faire émerger de nouvelles idées, proposez aux participants de formaliser ce qui ressort de l'atelier en consultant la section suivante.

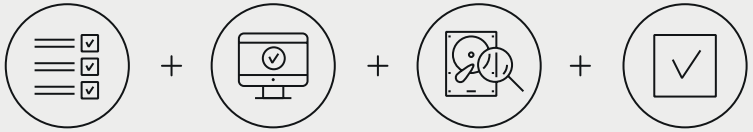
N'hésitez pas à ordonnancer dès ce premier atelier les grandes étapes qui guideront votre démarche de sécurité numérique. Si celle-ci s'inscrit dans une homologation de sécurité, consultez la section *« Se préparer à une démarche d'homologation »* page 31.

/ Un exemple suivi pas à pas : Le.Taxi

Afin d'illustrer concrètement la démarche proposée, nous avons choisi de rendre compte du premier cas réel dans lequel elle a été utilisée. Il s'agit de la plateforme nationale Le.Taxi dont la mission est d'informer sur la disponibilité et la géolocalisation des véhicules des opérateurs de taxi participants.

Pour ce système d'information, nous avons souhaité retracer dans ce guide l'ensemble de la démarche, du premier atelier à la constitution du dossier d'homologation. L'analyse de risque complète est disponible en fiche mémo page 49 et les exemples à suivre sont issus de ces ateliers et de leurs livrables.

/ Ressources utiles



Référentiels réglementaires et normatifs + Guides d'hygiène informatique + Bases de connaissances d'analyse de risque + Stratégie d'homologation visée

NOTES

4
LE PREMIER ATELIER
AGILITÉ & SÉCURITÉ NUMÉRIQUES

5 L'APPRÉCIATION DES RISQUES

L'APPRÉCIATION DES RISQUES : LES BASES À CONNAÎTRE ET À TRANSMETTRE

La valeur métier correspond à la valeur livrée aux utilisateurs et s'articule en *user stories*. Les *user stories* au niveau le plus macroscopique (parfois appelées *epics*) revêtent généralement un enjeu de sécurité significatif vis-à-vis de l'un ou l'autre des critères ci-dessous.

- **[D] Disponibilité :** la fonctionnalité peut être utilisée au moment voulu ;
- **[I] Intégrité :** les données sont exactes et complètes ;
- **[C] Confidentialité :** les informations ne sont divulguées qu'aux personnes autorisées ;
- **[P] Preuve :** les traces de l'activité du système sont opposables en cas de contestation.

De par leur criticité vis-à-vis des enjeux opérationnels et réglementaires de l'organisme, ces qualités doivent être protégées face aux menaces jugées vraisemblables (attaques informatiques, actes de fraude, erreurs, défaillances, etc.).

/ Exemple : Le.Taxi

User stories	[D]	[I]	[C]	[P]
Un client transmet son identifiant, sa position et son numéro de téléphone	●	●●	●●	
Un client peut émettre une demande (« héler virtuellement » un taxi)	●	●●	●	●
Un client peut évaluer une course effectuée ou déclarer un incident		●		●
Un administrateur peut enregistrer ou radier un taxi		●		●

● Besoin important ●● Besoin très important

/ DES BESOINS DE SÉCURITÉ AUX ÉVÉNEMENTS REDOUTÉS

Chaque besoin de sécurité identifié constitue le point de départ pour décrire un ou plusieurs événements redoutés susceptibles de compromettre la valeur d'usage.

/ Exemple : Le.Taxi

Événements redoutés	Impacts métier	Gravité
Le système ne répond pas	Expérience utilisateur dégradée ▸ Perte de clients	●
Un opérateur de taxis émet de fausses positions	Qualité de service dégradée ▸ Perte de clients	●
Un taxi fait une course d'approche en pure perte	Perte de confiance et d'adhésion des taxis ▸ Désengagement aboutissant à une réduction de l'offre de taxis	●●

● Modérée ●● Très élevée

/ LES RISQUES RÉSULTENT DE LA COMBINAISON DES ÉLÉMENTS DE L'ANALYSE

Un risque décrit la réalisation d'un scénario de menace intentionnel ou accidentel :

1/ une source de risque (un cybercriminel ou un fraudeur, par exemple)

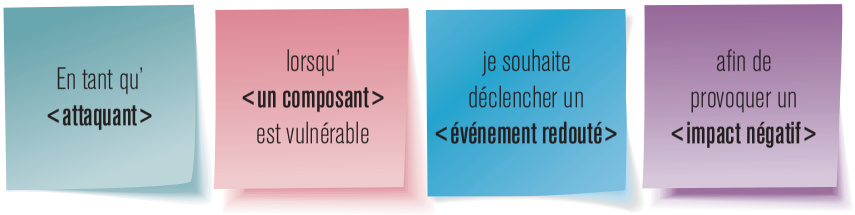
2/ par le biais d'un composant vulnérable du produit ou service

3/ provoque un événement redouté

4/ occasionnant des impacts sur la valeur métier, directs et indirects (humains, opérationnels, juridiques, etc.).

On lui associe une criticité basée sur l'estimation conjointe de la gravité des impacts et de la vraisemblance du scénario de menace conduisant à l'événement redouté.

Chacune des quatre catégories pré-citées correspondra à une couleur de Post-it. Voici une suggestion pour la correspondance entre les couleurs :



Commencez par ces quatre catégories qui ont tendance à constituer « l'angle mort » pour beaucoup d'équipes. Réservez une couleur plus classique, le jaune par exemple, pour lister séparément à la fin de l'exercice :

Les scénarios de risques peuvent être nommés *abuser stories* car ils correspondent au revers néfaste d'une *user story* et engendrent une perte de valeur.

5
L'APPRÉCIATION DES RISQUES : LES BASES À CONNAÎTRE ET À TRANSMETTRE
AGILITÉ & SÉCURITÉ NUMÉRIQUES

6 QUE FAIRE APRÈS CHAQUE ATELIER ?

QUE FAIRE APRÈS CHAQUE ATELIER ?

L'atelier initial ne suffira peut-être pas à placer l'équipe en situation de confiance vis-à-vis du traitement des risques numériques, particulièrement s'il s'agit de la première mise en œuvre d'une telle démarche ou d'un sujet particulièrement sensible.

Pour favoriser la continuité de ce travail d'un atelier à l'autre, il est utile d'en formaliser les résultats de manière cohérente avec la démarche agile choisie par l'équipe. Les détails dépendront, bien entendu, de chaque équipe et de ses pratiques d'organisation et d'ingénierie, mais voici quelques pistes :

- l'analyse de risque peut être consignée dans un Wiki ou tout autre espace documentaire, pourvu qu'il soit facilement accessible par tous les membres de l'équipe ;
- les *abuser stories* pourront être traitées comme les *user stories* et ajoutées au *backlog* ;
- si l'équipe le fait pour les *user stories*, elles peuvent être priorisées, annotées par leurs définitions de « fait » et éventuellement « prêt » ;
- la démonstration de la prise en compte des risques associés à une *abuser story* peut être faite par le biais de tests automatisés, comme c'est le cas pour les *user stories* : au lieu de démontrer par un test qu'un scénario fonctionnel aboutit, on cherchera à démontrer, au contraire, qu'un vecteur d'attaque n'aboutit pas.

7 LES ATELIERS SUIVANTS

LES ATELIERS SUIVANTS, ITÉRATION APRÈS ITÉRATION

Au fil des itérations, il deviendra périodiquement nécessaire d'actualiser ou d'affiner le résultat du premier atelier, par exemple lors des événements suivants :

- la réalisation d'une *user story* induit des évolutions d'architecture telles que l'ajout ou la modification d'un composant technique ;
- la réalisation d'une *user story* amène à exposer des données d'une autre nature que celles précédemment traitées (des données personnelles par exemple, alors que ce n'était pas le cas auparavant) ;
- l'équipe réalise un atelier dédié à une fonctionnalité spécifique du produit, qui adresse une ou plusieurs *user stories* plus particulièrement sensibles en termes de sécurité ;
- les retours des usagers amènent à évaluer différemment la valeur métier des différentes *user stories* ou les besoins de sécurité qui leur sont associés ;
- le nombre d'usagers ou le volume de transactions métier a sensiblement évolué, de telle sorte que l'exposition totale au risque a, elle aussi, évolué.

À l'image des autres activités menées par les équipes agiles, le travail à réaliser est alors presque identique à celui du premier atelier. Au fil des itérations, l'équipe apprendra ainsi à tenir compte, dans son plan de charge, du temps consommé par les activités liées à la sécurité afin de lisser ce travail dans le temps, comme elle le fait pour les activités liées à la qualité.

/ DETTE SÉCURITAIRE

On appelle « dette technique » le choix que fait une équipe de privilégier temporairement la livraison de nouvelles fonctionnalités, au détriment de pratiques de conception telles que le *refactoring*, l'automatisation en soutien du test ou la mise en commun des connaissances. Cette stratégie peut s'avérer payante mais doit résulter d'un choix délibéré et non d'un manque

de compétences dans ces domaines. L'intention est de mettre plus rapidement de nouvelles versions du produit ou du service entre les mains des usagers et d'obtenir des retours de ces derniers, avant de « rembourser » la dette dans un second temps.

Par analogie, on peut parler de « dette sécuritaire » lorsque l'équipe est amenée à différer le traitement de certains risques dans le but de mettre plus rapidement le produit à l'épreuve de ses premiers usagers. De la même façon, cette stratégie doit résulter d'un choix délibéré et non d'un manque d'attention portée à l'analyse de risques ou de compétences en la matière.

Dans les deux cas, un atelier d'analyse de risque tel que nous l'avons décrit ci-dessus peut amener l'équipe à réserver une part importante de sa capacité, ou consacrer une itération entière, à la prise en compte de la sécurité du système.

NOTES

7
LES ATELIERS SUIVANTS, ITÉRATION APRÈS ITÉRATION
AGILITÉ & SÉCURITÉ NUMÉRIQUES

8/

49/80

SE PRÉPARER À UNE DÉMARCHE D'HOMOLOGATION

SE PRÉPARER À UNE DÉMARCHE D'HOMOLOGATION

L'homologation de sécurité est un acte formel par lequel l'autorité responsable d'un système engage sa responsabilité en matière de gestion du risque. Elle est rendue obligatoire, pour les administrations, par le décret n° 2010-112 du 2 février 2010, selon des modalités précisées par le Référentiel général de sécurité (RGS). De même, elle est obligatoire pour tout produit traitant d'informations relevant du secret de la Défense nationale, comme précisé dans l'Instruction générale interministérielle 1300 (IGI 1300). Citons également la loi de programmation militaire, dont le volet *cyber* (loi n° 2013-1168 du 18 décembre 2013 - article 22), impose aux opérateurs d'importance vitale le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent, mené dans le cadre d'une démarche d'homologation.

Lorsqu'elle n'est pas réglementairement imposée, **la démarche d'homologation reste toutefois une excellente façon de témoigner, vis-à-vis des usagers, de la volonté de prendre en compte la sécurité numérique des services proposés et de valoriser le niveau de maîtrise des risques atteint** (la méthode présentée peut également servir de point de départ à une démarche de certification ou de qualification de solutions de sécurité).

Comme le rappelle le guide « *L'homologation de sécurité en neuf étapes simples* » :

> L'objectif de la démarche d'homologation [...] est de trouver un équilibre entre le risque acceptable et les coûts de sécurisation, puis de faire arbitrer cet équilibre, de manière formelle, par un responsable qui a autorité pour le faire.

Les livrables de l'atelier d'analyse de risque, tel que nous l'avons présenté dans ces pages, constituent un entrant nécessaire mais généralement insuffisant dans le cadre d'une démarche d'homologation. Par conséquent, nous recommandons de dédier un atelier à la préparation de la commission d'homologation (formalisation du dossier de sécurité, bilan des tests et audits de sécurité, consolidation des risques résiduels, suivi des mesures de sécurité et du plan d'action correctif).

/ HOMOLOGATION PROVISOIRE

Par hypothèse, l'équipe à laquelle s'adresse le présent guide cherche à mettre rapidement en service une première version incomplète du produit, puis à l'étoffer par incréments fonctionnels.

Dans ce contexte, l'équipe se dirigera donc naturellement vers **une décision d'homologation provisoire, afin d'adapter le niveau de risque résiduel accepté à un contexte donné.** Sa validité sera limitée dans le temps et conditionnée par des critères liés au volume ou à l'intensité d'exploitation, dans une unité appropriée : en nombre d'usagers, en volume de transactions, etc.

Ces **critères de validité** doivent pouvoir être mesurés et surveillés afin d'objectiver que l'on respecte encore les conditions de validité de l'homologation provisoire. L'équipe pourra moduler la durée et les critères de validité des homologations provisoires successives en fonction de la diffusion réellement constatée du service.

Une stratégie d'homologation pour la plateforme Le.Taxi pourrait ainsi se décliner en trois jalons :

- un jalon « *autorisation de tests* » d'une durée d'un à trois mois, menée exclusivement auprès d'usagers volontaires sur consentement explicite ;
- un jalon « *autorisation provisoire d'exploitation* », d'une durée maximale de 12 mois et un plafond de 1000 courses cumulées ;
- un jalon « *mise en service ferme* » tel que décrit ci-après.

/ HOMOLOGATION FERME

Une décision d'homologation ferme pourra être prononcée dès lors qu'un produit ou un service aura atteint son « régime de croisière ». Elle est généralement assortie d'une période de validité plus longue (trois ans étant une valeur typique) et vise le contexte d'exploitation normalement prévu, sans restrictions particulières d'usage.

Si l'équipe n'a pas eu recours aux services d'un expert en sécurité numérique lors des ateliers d'analyse de risque, ni à l'intervention d'un auditeur externe pour réaliser, par exemple, des tests d'intrusion ou une revue de code axée sur les besoins de sécurité, ces vérifications extérieures s'imposent généralement comme préalables à une décision ferme.

La mise en place d'un **plan d'amélioration continue de la sécurité** pour les versions successives à venir du produit ou du service est également un élément important de la décision d'homologation. Ce plan garantit la montée en puissance et en maturité de la sécurité du produit et permet une gestion priorisée des **risques résiduels** selon leur criticité.

Notez enfin que l'on prend soin de ne pas parler d'homologation « définitive ». En effet, le caractère évolutif d'un produit doté d'une forte composante logicielle impose de réévaluer périodiquement les risques, quand bien même le produit serait resté inchangé. Chose qui n'arrive, en pratique, que très rarement.

/ FORMALISER LE DOSSIER D'HOMOLOGATION

Le guide *L'homologation de sécurité en neuf étapes simples* détaille les étapes de la constitution du dossier de sécurité en vue d'une commission d'homologation. Simple, pratique et concis, l'expérience prouve qu'il sera un compagnon précieux pour toutes les équipes agiles qui souhaitent aboutir à une décision d'homologation.

À retrouver sur : www.ssi.gouv.fr

8/
SE PRÉPARER À UNE DÉMARCHE D'HOMOLOGATION
AGILITÉ & SÉCURITÉ NUMÉRIQUES

FICHE MÉMO 1 / STRUCTURER SA POLITIQUE DE SÉCURITÉ

La politique de sécurité d'un système d'information (PSSI) s'articule autour de trois niveaux de mesures de sécurité :

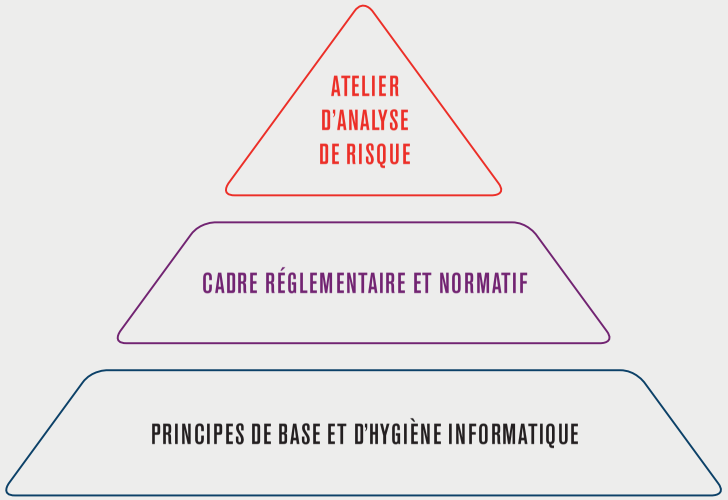
- **Les mesures d'hygiène informatique** couvrent divers domaines : sensibilisation et formation, authentification, sécurisation des postes et réseaux, administration, nomadisme, etc. Elles constituent un « socle de bonnes pratiques » applicables de façon systématique et conférant un niveau de protection capable de résister aux menaces les plus courantes.

- **Les mesures réglementaires et normatives** complètent ce socle d'hygiène par des exigences sectorielles applicables dans des domaines précis, selon les enjeux de sécurité identifiés (disponibilité, intégrité, confidentialité, preuve). Ainsi, la loi de programmation militaire (LPM) dicte-t-elle des obligations aux opérateurs d'importance vitale, le référentiel général de sécurité (RGS) s'applique aux systèmes d'information de l'administration, les règlements de la CNIL et le règlement général sur la protection des données (RGPD) européen s'appliquent à tout opérateur traitant de données à caractère personnel, l'instruction générale interministérielle 1300 (IGI 1300) définit les règles relatives à la protection du secret de la Défense nationale, etc.

- **Les mesures issues des ateliers d'analyse** de risque complètent ce socle par des mesures contextuelles, spécifiques aux cas d'usage du produit ou du service dans son écosystème (exemples : mise en place d'une liste blanche pour sécuriser un processus de traitement automatisé, durcissement d'une mesure d'hygiène, adaptation d'une mesure réglementaire, etc.). Ces mesures confèrent au produit robustesse et résilience face aux menaces ciblées et/ou sophistiquées jugées vraisemblables.

L'analyse de risque n'a donc pas vocation à procéder à une nouvelle identification des mesures de sécurité connues ou imposées, qui relèvent respectivement de l'hygiène et de la règlementation.

Structuration des mesures de sécurité d'un produit



FICHE MÉMO 2 / LES CLÉS POUR IDENTIFIER LES RISQUES NUMÉRIQUES CRITIQUES

Les activités de sécurité visent à identifier les scénarios de risques critiques et les mesures de sécurité permettant de les traiter. L'objectif est d'atteindre un niveau de sécurité correspondant aux enjeux et besoins sécuritaires dans une démarche agile, un scénario de risque est décrit sous la forme d'une *abuser story* de nature intentionnelle ou d'un scénario d'origine accidentelle. Cette fiche mémo recense les aspects méthodologiques à considérer en priorité lors des ateliers d'analyse de risque.

User story, abuser story et scénario accidentel

User story **:** *« En tant qu'utilisateur, je réserve en ligne mon billet de spectacle. »*

Abuser story (scénario intentionnel) : *« En tant qu'hacktiviste, j'empêche les clients de réserver en ligne leur billet de spectacle en saturant le serveur applicatif par une attaque en déni de service. Ceci conduit à un impact préjudiciable sur l'image et la crédibilité du gestionnaire du service, voire une perte de clients. »*

Scénario accidentel : *« Le service de réservation en ligne est rendu indisponible en raison d'une erreur de mise à jour du serveur applicatif par le prestataire en charge de la maintenance du système. Ceci conduit à un impact préjudiciable sur l'image et la crédibilité du gestionnaire du service, voire une perte de clients. »*

/ SE CONCENTRER SUR LES RISQUES NUMÉRIQUES LIÉS AUX CAS D'USAGE DU PRODUIT

L'analyse de risque doit s'attacher à identifier les *abuser stories* spécifiques, c'est-à-dire significatives en termes d'impact et qui relèvent de menaces – intentionnelles ou accidentelles – non couvertes par les mesures d'hygiène informatique ou réglementaires. Ces *abuser stories* permettent de compléter, d'orienter et de consolider la politique de sécurité du produit ou du service.

En termes de volumétrie, l'identification et le traitement de cinq à dix *abuser stories* constituent une première base solide pour définir les mesures de sécurité structurantes liées aux cas d'usage courants du produit.

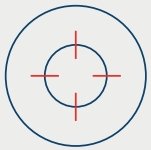
L'analyse de risque n'a pas vocation à identifier de nouvelles mesures de traitement connues ou imposées, qui relèvent respectivement de l'hygiène informatique et de la réglementation, et qui sont considérées comme nativement intégrées dans la politique de sécurité du produit (voir fiche mémo page 35). En revanche, elle a vocation à :

- valider ou non les dérogations éventuelles à ce socle de sécurité ;
- identifier le besoin de durcir ce socle ;
- identifier des mesures complémentaires *ad hoc* liées aux conditions d'emploi du produit, à ses processus métier, à son écosystème, etc.

/ PRIVILÉGIER LES *ABUSER STORIES* (SCÉNARIOS INTENTIONNELS)

Parmi les scénarios de risques à prendre en compte dans une analyse de risque, ceux de nature intentionnelle peuvent s'avérer particulièrement redoutables lorsque l'attaque est menée avec la volonté d'atteindre l'objectif visé en engageant des moyens particulièrement importants. Les éléments constitutifs classiques à prendre en compte dans une *abuser story* intentionnelle sont les suivants :

Un ou plusieurs attaquant(s)



Une cible

Un chemin d'attaque exploitant généralement plusieurs vecteurs et/ou vulnérabilités

Une ou plusieurs finalité(s)

La réussite d'une attaque sur un système d'information ne relève que rarement de l'exploitation d'une seule faille. Les attaques intentionnelles suivent généralement une démarche séquencée exploitant de façon coordonnée plusieurs vulnérabilités de nature informatique ou organisationnelle. C'est en raison de telles séquences que des failles d'apparence anodine peuvent devenir lourdes. Plusieurs modèles existent et peuvent être utilisés (exemple : *cyber kill chain* de Lockheed Martin). L'équipe pourra exploiter le modèle suivant, donné à titre d'information.

1 Reconnaissance externe

L'attaquant recueille des informations sur la cible par tous les moyens possibles : sources ouvertes (réseaux sociaux) ou non (officines).

2 Intrusion

L'attaquant s'introduit via un courriel piégé, un maliciel, des droits usurpés, une injection SQL, une faille non corrigée, un zero-day, etc.

3 Reconnaissance interne

L'attaquant mène des activités de reconnaissance interne lui permettant de cartographier l'architecture réseau, identifier les mécanismes de sécurité mis en place, recenser les vulnérabilités exploitables et localiser les services, informations et composants stratégiques.

4 Latéralisation et élévation de privilèges

À partir de son point d'accès initial, l'attaquant va progresser dans le système d'information et acquérir des droits lui permettant de se déplacer « n'importe où » dans le réseau, de propager les outils malveillants et de maintenir son accès en toute discrétion.

5 Pilotage et exploitation de l'attaque

Selon les objectifs de l'attaquant : sabotage, altération de service, vol de données, fraude, falsification, détournement d'usage, usurpation d'identité, défiguration de site, etc.

9 FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

Nous vous recommandons d'adopter une vision globale des séquences d'attaques possibles dans vos ateliers de sécurité, afin de ne pas minimiser à tort un scénario dont la vraisemblance et l'impact pourraient se révéler disproportionnés. Cette approche doit vous permettre d'identifier facilement les composants critiques susceptibles de servir de vecteurs d'entrée ou d'exploitation, de relais de propagation, etc. Ces composants – de nature technique, humaine ou organisationnelle – feront alors l'objet de mesures *ad hoc* ou d'un durcissement du socle existant

/ CONSIDÉRER L'ÉCOSYSTÈME COMME UNE SOURCE DE RISQUE POTENTIEL

On entend par écosystème l'ensemble des parties prenantes qui gravitent autour du produit ou du service et qui sont généralement nécessaires à son fonctionnement. Un nombre croissant de modes opératoires d'attaques exploite les vulnérabilités d'un écosystème pour atteindre leur cible. C'est ainsi qu'aux États-Unis, un casino a fait les frais d'une attaque menée par le biais… d'un aquarium connecté ! L'analyse de risque doit alors prendre en compte ces éléments de l'écosystème, susceptibles de rendre possible ou de faciliter la réalisation d'*abuser stories*.

/ Exemple

Injection de code malveillant par rebond via un partenaire tiers connecté facilitant l'exfiltration de données sensibles, etc.

Les parties prenantes critiques d'un écosystème, à prendre en compte dans l'analyse de risque, peuvent par exemple être identifiées en vous posant les questions suivantes :

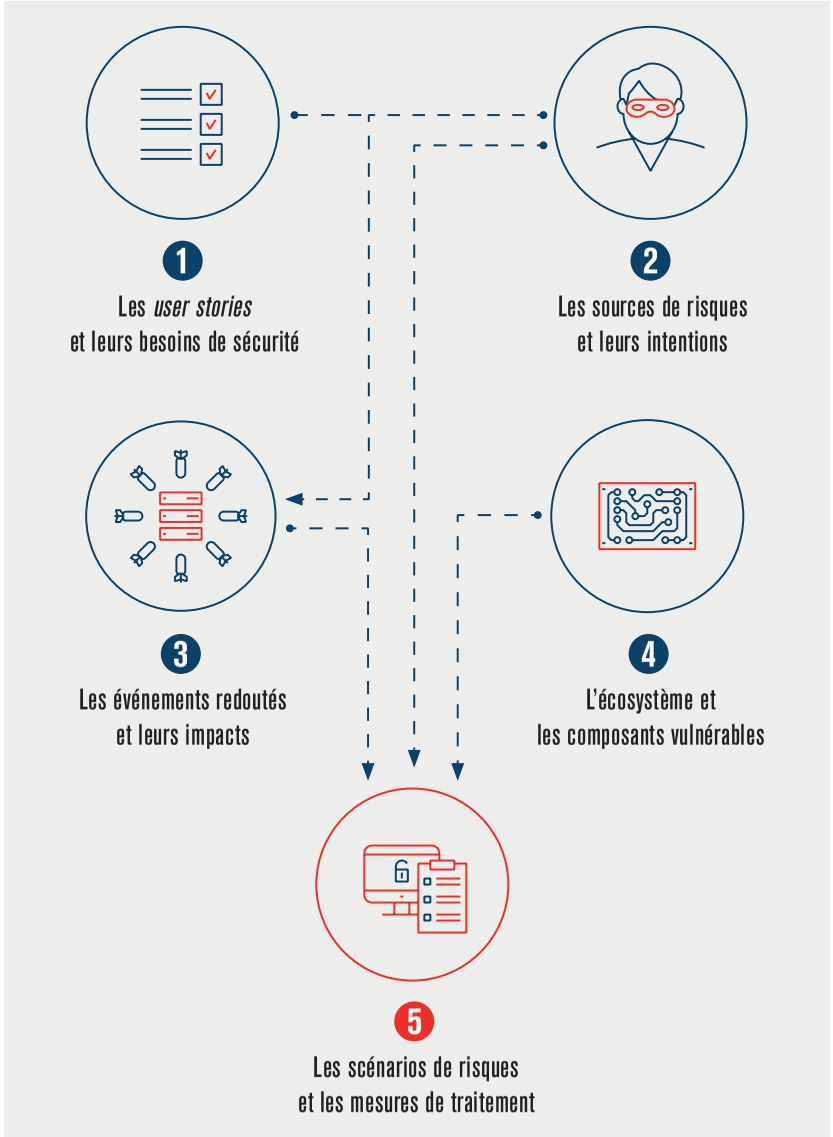
- La relation avec cette partie prenante est-elle essentielle pour mon activité ? Suis-je dépendant de services ou de bases de données hébergés ou exploités par la partie prenante ?
- Jusqu'à quel point la partie prenante accède-t-elle à mes ressources internes (mes locaux, mes réseaux informatiques, mon organisation) ?
- Ses services et réseaux informatiques sont-ils exposés sur Internet ? Sont-ils suffisamment sécurisés ?
- Puis-je considérer que ses intentions sont favorables à mon égard ?

Une méthode simple et pragmatique d'évaluation de la menace d'un écosystème est proposée dans le guide EBIOS de l'ANSSI.

L'identification des scénarios de risque, particulièrement ceux de nature intentionnelle, nécessite une certaine expertise en sécurité numérique. Un constat d'autant plus vrai pour les cas d'attaques sophistiquées, mettant en œuvre un séquencement planifié de modes d'action sur plusieurs composants – techniques et humains généralement – du produit et de son écosystème. Comme nous l'avons précisé plus haut, l'accompagnement de l'équipe par un expert dans ce domaine peut donc être un atout pour la réussite de l'atelier, en proportion avec le degré de complexité du produit et de l'écosystème.

9 FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

FICHE MÉMO 3 / LE CANEVAS DE L'ANALYSE DE RISQUE



❶ / LES *USER STORIES* ET LEURS BESOINS DE SÉCURITÉ

Dans cette rubrique, il s'agit de recenser les principaux éléments de valeur d'usage mis en œuvre par le produit, et d'estimer leurs besoins de sécurité (DICP : disponibilité, intégrité, confidentialité, preuve). Ces éléments seront généralement exprimés sous forme de *users stories.*

L'objectif est d'identifier, pour chaque *user story*, quels sont les besoins de sécurité les plus importants afin d'orienter par la suite le travail d'identification des scénarios de risques pertinents. Le degré d'importance peut être pondéré par un indice simple. Par exemple, **• pour un besoin important et •• pour un besoin très important.** Un schéma similaire pourra être adopté pour les autres éléments de l'analyse. L'évaluation de l'importance d'un besoin de sécurité est souvent itérative et obtenue par comparaison au fur et à mesure de l'atelier ; un besoin identifié comme « très important » traduit le fait qu'il est essentiel pour le produit.

Le point de départ de l'atelier – les *user stories* – est essentiel. En commençant par là, l'équipe ancre dans le reste de l'atelier l'idée que les mesures de sécurité servent la valeur livrée aux usagers. En effet, pour chaque besoin de sécurité important relatif à une *user story*, il y a un ou plusieurs événements redoutés et au moins un scénario de risque susceptible de compromettre la proposition de valeur.

/ Exemple

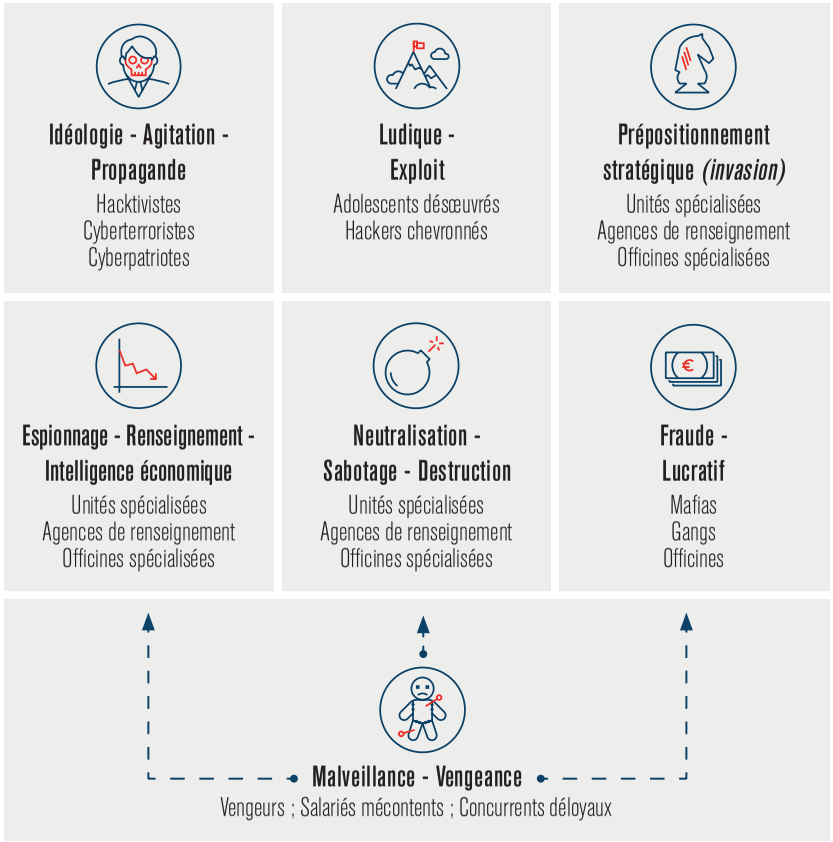
Un client peut émettre une demande (« héler virtuellement un taxi »), évaluer une course effectuée ou déclarer un incident.

9
FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

❷ / LES SOURCES DE RISQUES ET LEURS INTENTIONS

Il s'agit de recenser les sources de risques – accidentelles ou intentionnelles, externes ou internes – susceptibles d'impacter la valeur d'usage : qui ou quoi pourrait porter atteinte aux besoins de sécurité. Le schéma ci-dessous résume quelques-unes des motivations à l'origine d'attaques intentionnelles, et peut constituer un point de départ intéressant à la discussion lors de l'atelier.

/ Identification des sources de risques



Il est recommandé de recenser des sources de risques de natures et de motivations variées pour disposer d'un échantillon de risques représentatif à partir duquel bâtir des scénarios dont les menaces et modes opératoires diffèrent.

/ Exemple

- Opérateur concurrent cherchant à discréditer, voire saboter le service Le.Taxi (malveillance).
- Mafia cherchant à collecter des données à caractère personnel pour les monnayer (appât du gain).

❸ / LES ÉVÉNEMENTS REDOUTÉS ET LEURS IMPACTS

Un événement redouté (ER) correspond au non-respect d'un besoin de sécurité : chaque besoin de sécurité associé à une *user story* de l'étape ❶ se décline donc selon un ou plusieurs événements redoutés. Il convient de préciser les impacts (sur les missions ou la sécurité des personnes, financiers, juridiques, d'image, environnementaux, etc.) ainsi que le niveau de gravité estimé, l'objectif étant d'identifier en priorité les événements redoutés dont les conséquences seraient difficilement surmontables.

En première approche, l'échelle de cotation adoptée peut se limiter à un indice de priorité (P), par exemple : P1 – ER à retenir, P2 – ER à considérer dans un second temps. De façon plus élaborée, une échelle de cotation à trois niveaux ou plus pourra être adoptée : • **gravité faible,** • • **moyenne,** • • • **élevée**.

Un événement redouté est exprimé sous la forme d'une expression courte qui permet de comprendre facilement le préjudice lié à la *user story* concernée. Il est recommandé de mentionner dans l'intitulé de l'ER la source de risque la plus vraisemblable susceptible d'en être à l'origine. Enfin, dans un souci d'efficacité, l'équipe s'intéresse en première approche aux événements redoutés associés aux besoins de sécurité « très importants ».

/ Exemple

- Un opérateur concurrent, se faisant passer pour un client, hèle un taxi qui réalise une course d'approche en pure perte.

9 FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

❹ / L'ÉCOSYSTÈME ET LES COMPOSANTS VULNÉRABLES

Il s'agit d'identifier parmi les composants du produit ceux contribuant à la réalisation des *user stories* identifiées dans l'étape ❶ et susceptibles d'être concernés ou ciblés par les sources de risques de l'étape ❷. Il est recommandé de préciser, pour chaque composant, quelles sont les vulnérabilités que ces sources de risques pourraient exploiter.

/ Exemple

- Base de données Le.Taxi (vulnérabilités exploitables : accès en lecture/écriture depuis Internet, modification fréquente).

L'identification des composants peut être structurée comme suit :

- **infrastructures physiques :** bâtiments, locaux, espaces physiques permettant l'activité et les échanges de flux ;
- **organisations :** structures organisationnelles, processus métiers et supports, ressources humaines ;
- **systèmes numériques matériels et logiciels :** systèmes informatiques et de téléphonie, réseaux de communication.

Le degré de granularité dans la description des composants sera adapté au niveau de connaissance du produit lors de l'atelier. Enfin, les composants prioritaires à recenser sont ceux qui contribuent (de façon directe ou indirecte) aux *user stories* ayant des besoins de sécurité « importants ».

Afin d'étendre le périmètre de l'appréciation des risques, vous pouvez compléter cette étape en identifiant quelles parties prenantes de l'écosystème seraient susceptibles d'être exploitées pour faciliter une attaque sur un composant du produit (reportez-vous à la fiche mémo précédente). Les parties prenantes critiques à considérer en priorité sont celles qui ont un lien avec un des composants recensés.

/ Exemple

- Prestataire informatique assurant la télémaintenance du serveur qui héberge la base de données Le.Taxi.

❺ / LES SCÉNARIOS DE RISQUES (*ABUSER STORIES*) ET LES MESURES DE TRAITEMENT

La finalité de l'atelier est d'identifier les risques numériques de référence à prendre en compte pour bâtir ou compléter la politique de sécurité du produit.

L'équipe commence par dresser une liste de **scénarios de risques** – *abuser stories* – en confrontant les sources de risques ❷, les événements redoutés ❸ et les composants vulnérables ❹. Concrètement, il s'agit de voir de quelle façon chaque source de risque retenue peut impacter des composants du produit, par exploitation notamment de leurs vulnérabilités ou d'un facteur externe aggravant, pour générer un événement redouté. Chaque *abuser story* peut ensuite être évaluée en termes de vraisemblance puis de criticité à partir de la gravité de l'événement redouté associé.

/ Exemple

- Un attaquant externe accède aux informations à caractère personnel de clients en usurpant l'identité du serveur Le.Taxi ou en exploitant une vulnérabilité non corrigée.
- Un client de mauvaise foi attribue abusivement une mauvaise note à un taxi.

Pour chaque *abuser story* répertoriée, l'équipe peut définir si besoin **l'option de traitement du risque** la plus appropriée (éviter, réduire, transférer, accepter). Dans le cas où le risque doit être réduit, les participants identifient les **mesures de sécurité** complémentaires qu'il faudra mettre en œuvre, en plus des mesures existantes ou déjà prévues. Leur réalisation est consignée par l'équipe au même titre que les autres *user stories*.

9 FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

Enfin, l'équipe peut clore l'atelier en identifiant les **risques résiduels.** Ces derniers concernent :

- les *abuser stories* non traitées (acceptées en l'état) ou seulement partiellement (mesures de sécurité mises en place, mais ne réduisant pas complètement ou suffisamment le risque) ;
- les *abuser stories* faisant l'objet d'un transfert du risque, lequel ne couvre généralement pas l'ensemble des impacts (exemple : l'assurance ne couvre pas l'atteinte à l'image) ;
- pour affiner, dans un deuxième temps : les besoins de sécurité de l'étape ❶ et les événements redoutés de l'étape ❸ non déclinés en *abuser stories*.

Un certain travail (souvent subjectif) de consolidation des risques résiduels est à effectuer par l'équipe afin de disposer d'un bilan à jour et reflétant l'état de maîtrise du risque numérique du produit. Les risques résiduels les plus significatifs seront en priorité recensés et mis en évidence. Par exemple, l'usage d'échelles de gravité, vraisemblance et criticité, associées à des seuils d'acceptation du risque, constituera une aide précieuse pour hiérarchiser les risques résiduels avec objectivité et cohérence. Notons enfin que ce bilan, enrichi au fil des ateliers d'analyse de risque, sera complété par d'éventuelles vulnérabilités résiduelles identifiées à l'issue des audits de sécurité.

De façon alternative, l'équipe peut choisir de différer l'identification et la consolidation des risques résiduels lors d'un atelier de synthèse dédié, notamment pour la préparation d'une commission d'homologation.

La section suivante présente l'intégralité de l'analyse de risque pour la plateforme Le.Taxi et vous permettra d'observer l'articulation des différents éléments présentés ici sur un cas pratique.

FICHE MÉMO 4 / UN EXEMPLE COMPLET

Voici, à titre d'illustration, l'exemple détaillé du service Le.Taxi développé par l'incubateur de services numériques de la DINSIC.

Les tableaux que nous livrons ci-dessous correspondent à la restitution formelle d'un des ateliers d'analyse de risque, sans ajout ni retouches autres que des évolutions de terminologie en cours de rédaction.

User stories	Besoins de sécurité
Un taxi peut remonter sa position via l'interface de programmation applicative (API)	**Disponibilité :** une position doit remonter sous cinq minutes **Intégrité :** altérations détectables
Un client et un taxi conviennent d'une course (scénario global décomposé en sous-scénarios ci-dessous) : ▸ Un client peut connaître les taxis à proximité (ou suivre un taxi en approche) ▸ Un client peut émettre une demande (« héler virtuellement » un taxi) ▸ Le taxi, puis le client, peuvent confirmer la prise en charge ▸ Le taxi ou le client peut annuler la course	**Disponibilité :** sous cinq minutes **Intégrité :** altérations détectables et corrigeables **Confidentialité :** l'information sur les courses est à diffusion limitée
Un client peut évaluer une course effectuée ou déclarer un incident	**Disponibilité :** sous 72 h
Un taxi peut signaler un problème lié à une course	**Disponibilité :** sous 72 h
Un partenaire peut enregistrer un véhicule	**Disponibilité :** sous 72 h **Intégrité :** altérations détectables
Un administrateur peut enregistrer ou radier un partenaire	**Disponibilité :** sous 72 h **Intégrité :** altérations détectables
Un administrateur peut consulter les statistiques partenaires	**Confidentialité :** les statistiques sont à diffusion limitée

9 FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

FICHE MÉMO 4 / UN EXEMPLE COMPLET

Sources de risques	Modes opératoires	Vraisemblance
Attaquants externes (clients, *hackers*)	Un attaquant externe accède à la base de données	●
	Un attaquant externe surcharge le système	●●
Acteurs agréés de mauvaise foi (taxis, opérateurs)	Un partenaire surcharge le système	●●
	Un partenaire tente de fausser la concurrence en envoyant de fausses positions	●

Événements redoutés	Impacts métier	Gravité
Le système ne répond pas	**Expérience utilisateurs dégradée** ▸ **perte de clients**	●
Un opérateur de taxis émet de fausses positions	**Qualité de service dégradée** ▸ **perte de clients**	●
Un taxi fait une course d'approche en pure perte	**Perte de confiance et d'adhésion des taxis** ▸ **désengagement aboutissant à une réduction de l'offre de taxis**	●●
Un taxi s'enregistre avec de fausses informations	**Captation abusive de courses** ▸ **perte de confiance, risque juridique**	●

Composants du système
API Taxi Exchange Point (TXP)
Serveurs (1 serveur actuellement)
Données stockées
Administrateurs
Partenaires

Risques	Mesures existantes ou prévues
Un partenaire tente de fausser la concurrence en envoyant de fausses positions	Signature cryptographique des remontées de positions par les partenaires
Un attaquant externe accède à des informations confidentielles en exploitant une faille	Fermeture des ports autres que HTTP/HTTPS au trafic issu d'adresses IP inconnues
Un attaquant externe accède à des informations confidentielles en usurpant l'identité du serveur	Échanges sécurisés par HTTPS
Un client de mauvaise foi commande un taxi sans intention d'honorer sa commande	Transaction en deux étapes, bannissement temporaire des clients abusifs
Un taxi fournit des courses ne respectant pas la qualité de service attendue	Enregistrement d'une notation attribuée par le client au taxi
Un client de mauvaise foi attribue abusivement une mauvaise note au taxi	Les notations sont associées à une course réelle spécifique

9 FICHES MÉMO
AGILITÉ & SÉCURITÉ NUMÉRIQUES

FICHE MÉMO 4 / UN EXEMPLE COMPLET

Les risques résiduels suivants sont provisoirement acceptés mais doivent être traités par les mesures citées en regard :

Risques résiduels majeurs	Mesures à prendre
Le système est indisponible suite à un déni de service	Redonder les serveurs
Un taxi usurpe l'identité d'un véhicule légitime	À instruire lors de la montée en puissance

NOTES

9/ FICHES MÉMO

AGILITÉ & SÉCURITÉ NUMÉRIQUES

ANNEXES

GLOSSAIRE

Termes	Définitions
Abuser story	Brève description d'un scénario de risque (sous une forme analogue à celle d'une *user story*) qui sera utilisé pour déterminer les mesures de sécurité à implémenter et réaliser les tests de couverture du risque.
Analyse de risque	Sous-processus de gestion des risques visant à identifier, analyser et évaluer les risques.
Backlog	Liste de fonctionnalités ou de tâches (cf. *user stories*) jugées nécessaires à la bonne réalisation du produit.
Besoin de sécurité	Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à une valeur métier pour un critère de sécurité donné (disponibilité, confidentialité, intégrité, preuve, etc.).
Composant du système d'information (bien support)	Ressource sur laquelle reposent des fonctionnalités et qu'il convient de sécuriser en fonction de sa criticité. On distingue notamment : les systèmes numériques, les organisations et ressources humaines, les locaux et infrastructures physiques.
DevOps	Désigne une communauté réunie autour de pratiques visant à réduire l'écart entre les personnes qui développent un produit ou un service, et celles qui sont chargées de l'héberger, l'opérer, le surveiller, etc. Par exemple, les équipes de développement sont alertées et mobilisées sur tous les incidents de production.
DICP	Acronyme désignant les différentes catégories de besoins de sécurité qu'il convient usuellement de prendre en compte lors d'une analyse des risques numériques : disponibilité, intégrité, confidentialité, preuve.
Écosystème	Parties prenantes qui gravitent autour du système d'information (SI) et interagissent au travers d'interfaces logiques ou physiques. Il peut s'agir des clients ou usagers d'un service, de partenaires, de cotraitants, etc. L'écosystème inclut également l'ensemble des services et réseaux supports indispensables au bon fonctionnement du SI.
Événement redouté	Situation crainte par l'organisme. Il s'exprime par la combinaison des sources de menaces susceptibles d'en être à l'origine, d'une *user story*, du besoin de sécurité concerné et des impacts potentiels. Un événement redouté correspond à une violation d'un besoin de sécurité d'une *user story*.

Termes	Définitions
Homologation de sécurité	Attestation, par une autorité responsable, que le niveau de sécurité est conforme aux attentes et que les risques résiduels sont acceptables dans un contexte d'emploi donné.
Impact	Conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme ou sur son environnement.
Mesure de sécurité	Moyen de traiter un risque de sécurité. Une mesure peut être de nature technique, physique ou organisationnelle.
Objectif de sécurité	Dans le présent guide, un objectif de sécurité correspond à l'option de traitement décidée pour un scénario de risque. Typiquement : éviter, réduire, transférer, accepter.
Refactoring	Pratique technique consistant à améliorer la conception (lisibilité, modularité, etc.) d'un code source existant sans en modifier la fonctionnalité, et plus largement à prendre en compte la conception tout au long du développement d'un logiciel, plutôt que lors d'une phase distincte au début.
Risque résiduel	Risque subsistant après le traitement du risque et la mise en œuvre des mesures de sécurité. Il peut être présent dès la conception (l'équipe a accepté la présence du risque) ou identifié *a posteriori* (par exemple lors d'un audit externe).
Scénario de risque	Scénario décrivant la survenue d'un événement redouté. Il combine les sources de risques susceptibles d'en être à l'origine, les composants du SI visés, des modes d'action opérés sur ces composants et les vulnérabilités exploitables pour qu'ils se réalisent. Dans le présent guide, un scénario de risque est également désigné sous l'appellation *« abuser story »*.
Source de risque	Entité ou personne à l'origine de scénarios de risque.
User story	Au lieu de faire l'objet d'un cahier des charges, la réalisation d'un produit par une équipe agile suppose de découper le travail à réaliser en incréments de valeur métier appelés *« user stories »*.
Valeur métier	Information ou processus jugé important pour l'organisme et qu'il convient donc de protéger. On appréciera ses besoins de sécurité. En démarche agile, la valeur métier est généralement exprimée sous la forme d'une *user story*.
Vulnérabilité	Caractéristique d'un composant du SI qui peut constituer une faiblesse ou une faille au regard de la sécurité numérique.

BIBLIOGRAPHIE

Les sources ci-après constituent un bon point de départ pour tout organisme souhaitant approfondir ses connaissances ou bâtir son propre référentiel en matière de démarche agile, de développement sécurisé ou de pratiques d'homologation. Cette bibliographie ne se veut pas exhaustive.

/ DÉMARCHE AGILE

- *Le manifeste agile* est le document « historique » et de fait incontournable pour qui souhaite maîtriser le sujet. Toute la littérature qui suit se répartit en deux catégories, des gloses sur le Manifeste et des retours d'expériences du terrain.
  www.agilemanifesto.org/iso/fr/manifesto

- *Le référentiel des pratiques agiles* de l'Institut Agile, avec le soutien de l'association Agile Alliance, vise un recensement des pratiques les plus répandues dans la communauté. On l'utilisera avec profit comme un glossaire étendu permettant d'éviter des incompréhensions : la littérature sur le sujet est en effet riche en jargon, souvent anglophone, qui déroute parfois les néophytes.
  www.referentiel.institut-agile.fr

- *Gestion de projet agile, avec Scrum, Lean, eXtreme Programming…* de Véronique Messager, propose aux personnes ayant le rôle – formel ou informel – de chef de projet un tour d'horizon, tenant compte des spécificités du contexte français, de l'historique des démarches agiles et des principales ruptures avec les doctrines antérieures de gestion de projet. Il s'appuie sur les témoignages de nombreux experts issus de la communauté agile francophone.

- *The Phoenix Project,* de Gene Kim, Kevin Behr et George Spafford est une bonne introduction à l'un des domaines les plus récemment développés par la communauté agile : les principes et pratiques regroupées sous l'étiquette DevOps. Sous une forme inédite (c'est un roman), il constitue une entrée en matière accessible et efficace.

ANNEXES

AGILITÉ & SÉCURITÉ NUMÉRIQUES

/ DÉVELOPPEMENT SÉCURISÉ

Vous trouverez sur le **site de l'ANSSI** un ensemble de guides, recommandations et bonnes pratiques (cryptographie, postes de travail et serveurs, liaisons sans fil et mobilité, réseaux, applications Web, externalisation, systèmes industriels, technologies sans contact, archivage électronique, etc.) :
www.ssi.gouv.fr/entreprise/bonnes-pratiques

OWASP Proactive Controls (*Open Web Application Security Project*) propose une liste de dix contrôles de sécurité préventifs dédiés au développement logiciel. Ces techniques sont classées par ordre d'importance décroissant. Ce document a été écrit par des développeurs pour des développeurs :
www.owasp.org/index.php/OWASP_Proactive_Controls

SAFECode – Security Guidance for Agile Practitioners – propose des recommandations pratiques sous forme de *user stories* centrées sur la sécurité et les tâches de sécurité qu'ils peuvent facilement intégrer dans leurs environnements de développement agile :
www.safecode.org/publications

/ PRATIQUES D'HOMOLOGATION ET D'ANALYSE DE RISQUE

- **Guide ANSSI** *L'homologation de sécurité en neuf étapes simples* :
  www.ssi.gouv.fr/guide-homologation-securite

- **Base de connaissances EBIOS de l'ANSSI** :
  www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager

- Vous trouverez également sur le **site de l'ANSSI** d'autres guides vous permettant d'approfondir vos pratiques en matière par exemple de défense en profondeur, d'élaboration d'une PSSI ou d'un plan de montée en maturité SSI :
  www.ssi.gouv.fr/entreprise/bonnes-pratiques/methodologie

Outils pratiques pour l'identification et l'évaluation de scénarios de risque numérique (exemples) :

- *Tactical Threat Modeling* de SAFECode :
  www.safecode.org/publications

- *STRIDE Threat Model* de Microsoft :
  www.owasp.org/index.php/Threat_Risk_Modeling#STRIDE

- *DREAD Risk Rating Security Threats* :
  www.wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD
  ou www.owasp.org/index.php/Threat_Risk_Modeling#DREAD

/ RÉGLEMENTATION (DE SÉCURITÉ)

- Le lecteur pourra se reporter au site de l'ANSSI qui présente un panorama des textes réglementaires en matière de sécurité numérique relatifs à la protection des systèmes d'information, à la confiance numérique, ainsi que plus spécifiquement à la cryptographie ou à d'autres réglementations techniques :
  www.ssi.gouv.fr/entreprise/reglementation

- Concernant la sécurité numérique des systèmes d'information d'importance vitale (SIIV), régie par l'article 22 de la loi de programmation militaire, le lecteur pourra consulter le lien suivant :
  www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france

[...]

ANNEXES

AGILITÉ & SÉCURITÉ NUMÉRIQUES

DOSSIER : Sécurité informatique : comment se protéger ?

www.lagazettedescommunes.com/461392/former-et-sensibiliser-les-agents-a-la-securite-informatique-pour-reduire-les-risques

---

NUMÉRIQUE

Former et sensibiliser les agents à la sécurité informatique pour réduire les risques

Pierre-Alexandre Conte | Actu experts prévention sécurité | Dossiers d'actualité | Publié le 20/09/2016 | Mis à jour le 23/02/2017

Lorsque le sujet de la sécurité numérique est mis sur la table, les agents, qui adoptent encore trop souvent des comportements à risque, ont tendance à être exclus de l'équation. A tort, comme l'ont rappelé la plupart des intervenants du colloque organisé par la Mission Ecoter le 15 septembre, qui invitent les collectivités territoriales à former et sensibiliser leur personnel sur cette question.

Les acteurs du monde de la sécurité informatique s'accordent à le dire : une grande partie des incidents sont liés à une faille humaine. Une étude de l'Université Friedrich-Alexander d'Erlangen-Nuremberg menée par le professeur Zinaida Benenson et publiée mi-août a d'ailleurs révélé que 56% des personnes cliquent sur des liens présents dans des mails envoyés par des inconnus. Et ce, même si celles-ci ont conscience du danger qu'elles encourent. La curiosité est la principale raison de cette prise de risque.

Ce test effectué auprès de 1700 étudiants, Laurent Charveriat l'a relayé au cours d'un colloque organisé le 15 septembre à Puteaux par la Mission Ecoter. Le thème de celui-ci : « Sécurité des lieux, sécurité des usagers. » Le directeur d'I-Tracing, une société notamment spécialisée dans la sécurité des systèmes d'information, souhaitait par ce biais faire comprendre aux collectivités territoriales qu'elles sont d'abord rendues vulnérables par le comportement de leurs agents.

Les agents en première ligne

Contrairement à ce que beaucoup d'entre elles pensent encore, comme l'a révélé en 2015 une étude de Primo France, les collectivités territoriales sont des cibles, à l'instar des particuliers ou des entreprises. Et elles le seront d'autant plus à l'avenir avec la place croissante prise par le numérique.

De l'atteinte à la vie privée au vol de données sensibles en passant par l'altération de la réputation ou les pertes financières, les conséquences d'un piratage peuvent être multiples, comme l'a rappelé Jean-Philippe Collignon, directeur de développement chez Engie Ineo Cybersécurité.
Pour diminuer le risque, la seule véritable réponse à apporter, c'est la formation. Il est devenu indispensable de sensibiliser les agents à ces questions pour les pousser à adopter un comportement responsable tout en leur

faisant prendre conscience des pratiques frauduleuses existantes. Car ces derniers sont plus que jamais en première ligne.

Début juin, la société PhishMe a publié un rapport établissant que 93% des attaques via phishing contenaient des ransomwares, soit des logiciels malveillants visant à prendre en otage des données en les cryptant et réclamer une rançon en échange de leur restitution. Un simple clic peut ainsi conduire un système d'information à être paralysé. C'est ce qui est arrivé à un hôpital de Los Angeles, en février 2016. Pour retrouver au plus vite un fonctionnement normal, la direction de ce dernier a dû débourser 17000 dollars. L'idée reçue veut que les hackers visent des cibles qui auraient des moyens financiers importants. Mais Laurent Charveriat rappelle qu'ils n'adoptent généralement pas cette stratégie-là : « Le maire a tendance à se dire que sa commune n'est la cible de rien, de personne. Mais la logique des hackers, c'est d'inonder partout. Statistiquement, il y a un nombre d'utilisateurs qui vont cliquer. »

De l'importance de connaître son système d'information

Si la faille humaine ne doit pas être négligée, il ne faut pour autant pas mettre de côté les autres portes d'entrée vers les systèmes d'information des collectivités territoriales. A commencer les lieux en eux-mêmes, dont la sécurité physique doit être assurée. Veiller à ce que les sous-traitants respectent les règles fixées est également indispensable.

Concernant le volet numérique, « cela ne sert à rien de tout sécuriser, cela n'a pas de sens », affirme le directeur général d'I-Tracing. Avant de préciser sa pensée : « On met des agents de police devant les écoles, pas partout. Et on ne commence pas par la technique. Il faut faire un 'Connais-toi toi-même'. Quelles sont les données sensibles et qui sont les consommateurs de ces données ? Uniquement des personnes en interne ou la population y a-t-elle accès ? Derrière, il faut les mesures qui s'imposent. »

Ces mesures dépendent donc essentiellement de ce qui est menacé. Certaine solutions permettent un retour rapide à un fonctionnement normal tandis que d'autres garantissent une perte minimale de données en cas de panne. Reste à savoir si l'outil met en cause le fonctionnement de la collectivité territoriale ou non. Par ailleurs, Audrey Paris, expert SSI chez Engie Ineo a pris soin de préciser qu'un « simple bilan ponctuel de la sécurité ne suffisait pas » mais qu'il fallait un « suivi en continu ».

Évidemment, cette sécurité a un coût. Mais elle est aujourd'hui devenue un enjeu central. Pour ceux qui se refusent encore à penser dans ce sens, le nouveau règlement européen sur la protection des données personnelles qui entrera en application en 2018 devrait achever de les convaincre. Les sanctions seront ainsi renforcées.

Certes, une marge de manœuvre est laissée aux États par rapport au secteur privé mais les amendes encourues par les entreprises – jusqu'à 20 millions d'euros ou de 2 à 4% du chiffre d'affaire – en cas de non respect des règles donnent un ordre d'idée des sanctions envisageables. Avant d'en arriver là, mieux vaut donc anticiper. Et

appliquer dans un premier temps ce que préconise l'ANSSI dans son référentiel général de sécurité.

numéro 09 fiche
SSI PRATIC
assuris.fr - janvier 2010

DOCUMENT 10

Prendre en compte et maîtriser le facteur humain dans la SSI

« Pour plus de sécurité, nous avions choisi de changer le mot de passe des utilisateurs tous les 6 mois. Mais cela n'a pas duré longtemps car les collaborateurs écrivaient leur code sur un papier qu'ils cachaient dans leur tiroir ou sous leur clavier.
Finalement cette mesure a créé des risques supplémentaires au lieu de mieux protéger notre système d'information. »

Même avec les meilleurs outils existants en matière de sécurité informatique, le système d'information d'une entreprise peut devenir perméable si l'entreprise ne maîtrise pas le facteur humain.
En effet, le personnel fait partie intégrante du SI. Il en est même un maillon essentiel. Chaque salarié ayant accès à tout ou partie du patrimoine informationnel, il est important qu'il ait conscience de la sensibilité et de la vulnérabilité des informations et qu'il respecte quotidiennement les règles internes de sécurité.

Cette fiche pratique vous explique comment sensibiliser le personnel à la sécurité informatique et pourquoi nommer un responsable dans ce domaine.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

POINTS CLES

Voici les points clés à retenir :

- Intégrer la protection de l'information dans la communication globale de l'entreprise.
- Sensibiliser, former, impliquer et responsabiliser le personnel à tous les niveaux.
- Communiquer sur la stratégie et les actions prévues en matière de sécurité, en insistant largement sur les bénéfices d'une telle démarche afin d'éviter les potentielles résistances aux changements.
- Assurer le responsable sécurité du soutien indispensable de la hiérarchie.
- Eviter que l'entreprise attende les problèmes pour agir, il est souvent déjà trop tard.
- Mettre en place des solutions réalistes et adaptées en fonction des risques encourus par l'entreprise.

Sommaire

1. Nommer un responsable « Sécurité du système d'information »

Le responsable SSI a pour mission de garantir l'intégrité, la confidentialité, la disponibilité et la traçabilité des données de l'ensemble des systèmes d'information de l'entreprise. Il définit les orientations, élabore et met en œuvre une politique de sécurité.
Il est aussi celui sur qui repose la maîtrise du facteur humain dans la sécurité du système d'information.

Il n'existe pas de profil type. Le responsable SSI doit réunir plusieurs compétences :

- Une bonne connaissance dans le domaine de la sécurité, sans pour autant connaître en détail le fonctionnement des technologies. Il doit acquérir et mettre à jour un minimum de connaissances à la fois pour être crédible vis-à-vis des techniciens en sécurité informatique et pour savoir apprécier les risques liés à l´utilisation du système d´information.

- Une vision transversale de l'activité de l'entreprise.

- Des aptitudes en communication pour mener des missions de sensibilisation.

- Des aptitudes en organisation car il sera le chef d'orchestre de la gestion d'éventuels sinistres.

Dans les PMI PME, cette fonction est très souvent assurée par le responsable informatique lui-même ou encore le responsable qualité.

2. Sensibiliser et former le personnel à la SSI

2.1. Comment ?

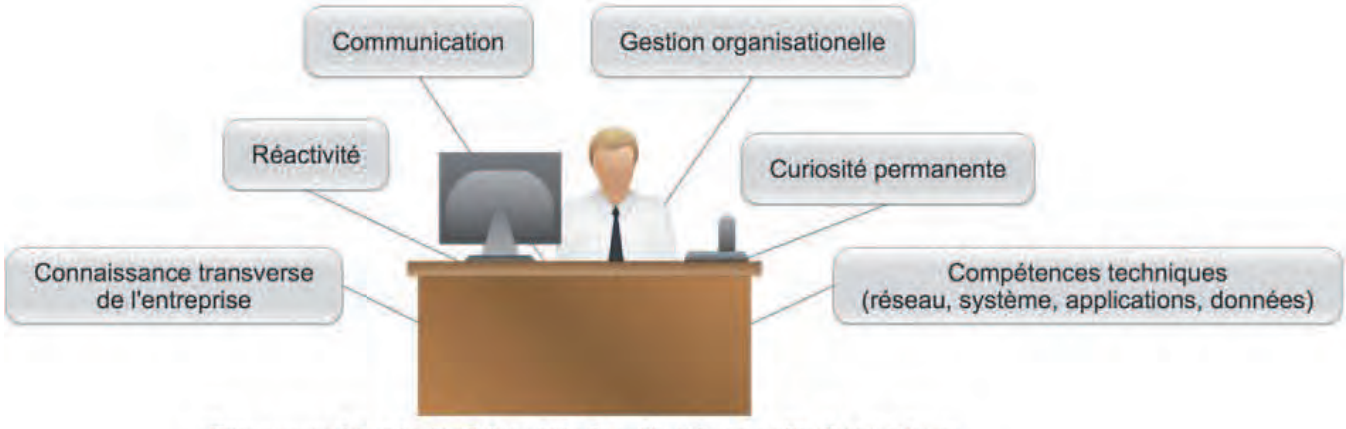
Il s'agit de mener régulièrement des actions d'information et de sensibilisation auprès du personnel pour lui faire comprendre les enjeux de la SSI. Ces actions facilitent l'acceptation et l'application de règles qui peuvent parfois paraître contraignantes.

L'objectif est de transmettre un premier niveau de connaissance et de diffuser les bonnes pratiques concernant la sécurité informatique.
Tout utilisateur doit :

- Avoir eu connaissance de la charte informatique et l'appliquer.
- Connaître la démarche à suivre en cas de problème de sécurité informatique (personne à contacter).
- Etre en mesure de juger de la sensibilité d'une information.
- Connaître son périmètre d'accès à l'information.

Les actions de sensibilisation peuvent se faire à travers :

- Des discussions informelles entre employés et responsables SSI.
- Des notes d'information (emails courts et pratiques).
- De l'affichage dans les zones sensibles (photocopieurs, bureau de recherche et développement).
- Des réunions thématiques régulières.
- Des séances de formation.



Responsable de la Sécurité des Systèmes d'Informations

2.2. Les facteurs clés de succès

Les supports utilisés dans le cadre d'actions de sensibilisation à la SSI doivent être simples, ludiques et interactifs afin d'assurer l'efficacité des messages et de susciter l'intérêt du plus grand nombre.

L'introduction de nouvelles pratiques peut générer certaines résistances aux changements. Il est alors conseillé d'axer le discours de sensibilisation sur les avantages qu'apporte la SSI pour garantir l'activité de l'entreprise.

Par ailleurs, il convient de contrôler régulièrement le respect par le personnel des règles et sa connaissance des dispositions pratiques inscrites dans le règlement intérieur. Des mesures incitatives peuvent aussi être envisagées.Généralement, les actions de sensibilisation se font en complément d'une démarche de diffusion de la charte informatique interne[1].
Enfin, les règles seront d'autant plus prises au sérieux si les responsables les respectent eux-mêmes de manière exemplaire.

[1] Pour en savoir plus sur la charte informatique, se référer à la fiche n°6 « Les droits et obligations du chef d'entreprise en matière de SSI ».

DOSSIER : Sécurité informatique : comment se protéger ?
www.lagazettedescommunes.com

Pierre-Alexandre Conte | Dossiers d'actualité | France | Publié le 27/02/2017

NUMÉRIQUE

« Cloud » et souveraineté numérique : le débat fait rage

Une note ministérielle du 5 avril 2016 affirme l'obligation pour les collectivités d'avoir recours à un « cloud souverain ». Mais l'offre répondant à cette injonction ne donne pas satisfaction à toutes les collectivités, qui se trouvent dans une position inconfortable.

Le « cloud » est une solution adoptée ou envisagée par un nombre important de collectivités. Elles voient dans ce système de stockage « dans le nuage », une solution adaptée à leurs besoins de modernisation. Le 5 avril 2016, une note informative émanant du ministère de l'Intérieur et du ministère de la Culture et de la communication est toutefois venue jeter le trouble.

Celle-ci explique que les collectivités doivent impérativement souscrire une offre de « cloud souverain ». La démarche inverse est qualifiée « d'illégale, pour toute institution produisant des archives publiques » du fait de la nécessité de s'assurer que les données sont stockées et traitées sur le territoire national.

Les Américains dans le viseur

A l'évidence, la note, qui a été signée par le directeur général des collectivités locales, Bruno Delsol, et par le directeur chargé des archives de France, Hervé Lemoine, vise les offres provenant de sociétés américaines.

De Microsoft à Google, en passant par Amazon, les entreprises proposant leurs services sont nombreuses. Elles disposent en effet de moyens colossaux et ont investi depuis longtemps dans ce système de stockage. A ce jour, ces acteurs sont nettement en avance sur leurs concurrents français et se taillent la part du lion sur le marché international et hexagonal.

Pour autant, adopter une solution émanant d'entreprises américaines comporte un risque. Et pas des moindres. Car ces dernières ont l'habitude de conserver des « backdoors », c'est-à-dire des portes dérobées dont les utilisateurs n'ont pas connaissance, qui leur permettent d'avoir un accès au logiciel.

Or en vertu des lois en vigueur aux Etats-Unis, le gouvernement peut avoir accès aux données personnelles hébergées sur le sol américain ou détenues par une société américaine à tout moment, sans autorisation judiciaire. Ce qui pose un problème évident pour les collectivités.

Offre étrangère

Si la note informative du 5 avril 2016 donne des consignes assez fermes, elle n'est, pour autant, pas un texte de loi. Aussi, malgré les risques encourus, les collectivités peuvent encore se tourner vers une offre de « cloud » étrangère. D'autant que plusieurs sociétés américaines, à l'instar d'Amazon et de Microsoft, ont annoncé qu'elles allaient ouvrir des « data centers » en France.

Leurs systèmes de stockage « en nuage » deviendront alors, de fait, souverains. Mais rien ne permet d'affirmer pour autant que les données détenues par ces entreprises ne tomberont jamais dans les mains de l'administration du pays dans lequel est établie leur maison mère. Les collectivités territoriales qui abordent la question du « cloud » se doivent donc d'être conscientes des conséquences induites par le choix de leur prestataire. Certaines d'entre elles vont ainsi privilégier l'efficacité du service en veillant à ne pas stocker de données sensibles, tandis que d'autres vont choisir la solution la plus sécurisée… Cette question n'a, de toute évidence, pas fini de faire parler.

Communauté urbaine de Dunkerque (Nord) 21 communes – 201 400 hab.

Une orientation vers une offre de Microsoft pour remplacer la messagerie actuelle

La cybersécurité fait partie des préoccupations principales de la communauté urbaine et de la ville de Dunkerque. Pour autant, en dépit de la note informative du 5 avril 2016, elle s'oriente vers une offre « cloud » de Microsoft pour remplacer sa messagerie actuelle sous Lotus notes.Un choix assumé par son directeur des systèmes d'information, René-Yves Labranche : « Une annonce de Microsoft nous a signalé que la société implanterait des data centers en France dès 2017. Et Office 365 semble être la solution adaptée à notre besoin, tout en respectant au maximum la sécurité », lance-t-il.

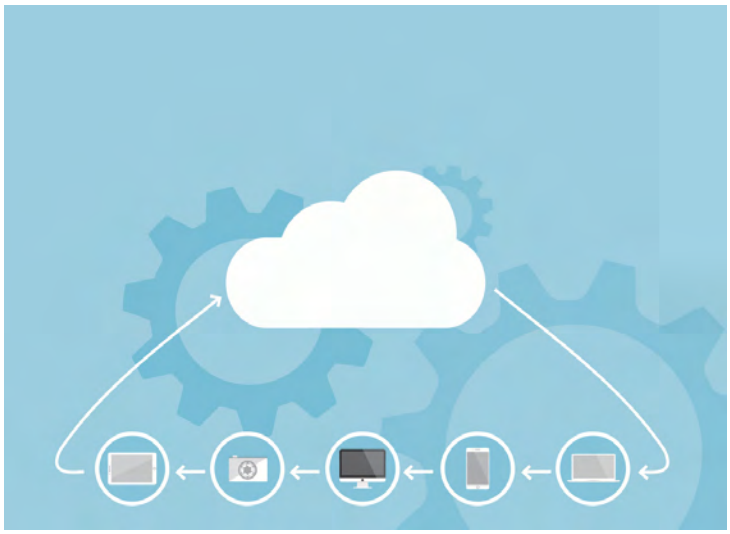
Avant d'expliquer en profondeur la démarche : « Il y a une antinomie entre la notion de cloud souverain et la nécessité de transformation et de modernisation des systèmes d'information dans les collectivités. Si on applique cette note à la lettre, on fait marche arrière sur la totalité de la transformation qu'on a déjà opérée et pour laquelle nous sommes en conformité avec le référentiel général de sécurité. Nous avons un RSSI et avons beaucoup investi en termes humains et financiers pour améliorer la sécurité de notre système d'information. »

REFERENCES

- Note d'information relative à l'informatique en nuage, 5 avril 2016

Le PRA et le PCA revisités par le Cloud

11 juin 2018



Dans toutes les branches d'activités, la continuité de la production informatique devient critique. Les plans de reprise se démocratisent autour des fibres noires, de la virtualisation et du Cloud.

« Sans plan de reprise ou de continuité informatique, l'organisation se ferme de nombreux marchés car désormais les appels d'offres réclament aux soumissionnaires qu'ils précisent

leurs moyens de secours informatiques mis en place. La technologie pousse dans le bon sens, vers la démocratisation des solutions. Les prix d'acquisition et d'exploitation chutent à travers les offres Cloud, la location de fibre noire ou encore les postes de travail en mode VDI », observe **Bruno Hamon**, fondateur et directeur associé du cabinet Mirca et chargé de mission à l'Afnor.

Le spécialiste préconise de définir avec les métiers les exigences de continuité d'activité, par rapport à la notion de "promesse client". Pour cela, il prend en compte trois sinistres principaux dans l'élaboration d'un PCA : des locaux inaccessibles, de façon durable ou non, une perte totale ou partielle du système d'information et un absentéisme important du facteur humain. Un tel plan doit *« se construire avec les métiers en y ajoutant la prévention contre les fuites de données et la nécessité d'être en conformité avec le Règlement sur la protection des données personnelles ou RGPD dans l'objectif de bien maîtriser son patrimoine informationnel. Cela inclut les données à caractères personnelles au-delà de son système d'information, dans le Cloud comme chez les hébergeurs. »*

> Bruno Hamon

Plusieurs risques à anticiper

Les technologies et prestataires de services Cloud relèvent le défi d'une production IT ininterrompue, autour d'offres DRaaS (Disaster Recovery as a Service) notamment : *« Depuis deux ans, les CSP (Cloud Service Providers) développent leur propre réseau d'interconnexion entre datacenters, sans passer par les opérateurs. La fibre noire multiplexée facilite ainsi la bascule rapide entre les sites de Paris et Francfort, en cas de sinistre »,* précise **Didier Lavoine**, directeur technique, Développement et Innovation de Digora.

> Didier Lavoine

On distingue trois types de pannes majeures intervenant au niveau des bâtiments, des équipements logiques ou physiques. Sur site, les incidents météorologiques (orage, grêle ou tempête) peuvent provoquer une coupure d'alimentation électrique, une inondation, un incendie, voire la destruction du datacenter. Un acte de vandalisme, de terrorisme ou une attaque militaire auront des conséquences semblables.

Les pannes de serveurs ou d'équipements réseau sont le plus souvent liées à un composant défectueux (processeur, mémoire, disque, carte réseau). Enfin les pannes

logiques ont diverses causes possibles : la cyberattaque, l'effacement maladroit de fichier, un bug dans une application ou la corruption de données numériques.

Face à cette variété de sinistres, l'organisation retient souvent plusieurs protections pour limiter l'impact des défaillances. Ce faisant, elle multiplie les interfaces d'administration à prendre en main en situation d'urgence. Le PRA détaille les procédures pour remettre en production les systèmes critiques, pas à pas. Il précise les étapes clés à suivre en cas de crash. Pour le préparer, on place trois repères clés sur une échelle de temps, à commencer par l'heure supposée du sinistre au centre de cette ligne. Deux jalons sont répartis de part et d'autre : à gauche, la PDMA (perte de données maximale admissible) et à droite du sinistre, la DMIA (durée maximale d'interruption admissible) ou DIMA (durée d'indisponibilité autorisée). Ces deux repères peuvent glisser dans le temps, selon la criticité de l'application. Ils s'expriment en minutes, en heures ou en jours, plus rarement en secondes.

Des objectifs propres à chaque plan

Chaque plan de reprise d'activités gagne à établir ses propres objectifs, réalistes, par application. Cette approche fournit la séquence de restauration des applications et données à remettre en production, suivant leur priorité. Dès qu'une nouvelle application apparaît, l'évaluation de son couple PDMA/ DMIA devient nécessaire. De même, tout nouvel équipement actif à peine connecté, un serveur, un firewall ou un routeur rejoindra la liste des matériels à remplacer dans un délai convenu, par une ou plusieurs voies planifiées d'avance (acquisition, échange ou stock).

Un nouveau socle tangible à définir

Lorsqu'un sinistre survient, le temps de réaction de l'organisation conditionne la reprise des activités métiers, donc la poursuite des affaires. *« Le PRA n'est pas un simple effet de mode. La dépendance des entreprises au digital est de plus en plus forte,* souligne **Anwar Saliba**, directeur général adjoint d'Euclyde. Le coût de mise en œuvre du plan ne serait pas son principal obstacle : *« Les technologies Cloud allègent le coût du PRA, lorsqu'on réserve des ressources sur un site distant, on ne paye qu'en cas de besoin. Nos clients consacrent de 5 % à 10 % de leur budget IT annuel à leur PRA. C'est peu, comparé aux 50 % nécessaires pour un PCA, bâti sur deux datacenters distincts. »*

La mutualisation des moyens techniques et le modèle de facturation du Cloud, à l'usage, expliquent la démocratisation du PRA, assuré par une bonne gestion du capacity planning par le prestataire. En effet, la probabilité que tous ses clients

déclenchent leur PRA en même temps reste proche de zéro. L'investissement se transforme donc en charges : *« Tant que le client ne démarre pas son PRA, il n'y pas de licence à payer aux fournisseurs ; seules des ressources matérielles sont mises à disposition ».*

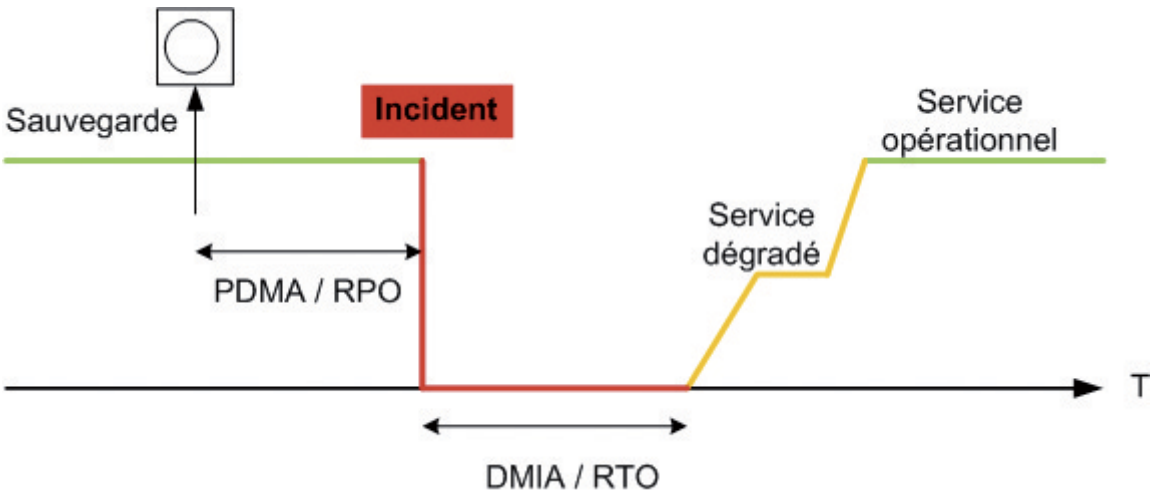
> Anwar Saliba

En résumé, la définition du PRA dépend des objectifs de sécurité que l'organisation se fixe : *« Lorsqu'une reprise sous un à cinq jours convient, une simple sauvegarde suffit. Mais si on doit assurer une restauration complète sous 4 heures, il faut ajouter des mécanismes de réplication synchrone et quelques zéros à la facture »,* reconnaît-il. Pour reconstruire certaines transactions critiques, on peut aussi repartir de snapshots ou rejouer les dernières étapes des journaux systèmes.

Plus que des recettes de virtualisation ou d'automatisation, le socle d'infrastructure doit devenir tangible et résilient.

Le mécanisme de reprise d'activités

PDMA Perte de données maximale admissible
RPO Recovery point objective, objectif quantitatif de données perdues
DMIA Durée maximale d'interruption admissible
RTO Recovery time objective, objectif de reprise après incident



AVIS D'EXPERT

Francis Brisedoux,
manager IT d'ASL Airlines France.

ASL Airlines France retient Rubrik pour ses restaurations instantanées

« Ceinture, bretelles et parachute », qualifie **Francis Brisedoux**, le manager IT d'ASL Airlines France. La compagnie aérienne, héritière de l'Aéropostale, protège efficacement le socle informatique de ses activités de fret et de transport de passagers, assurées par la rotation de 17 Boeing 737.

Elle a choisi le soutien de l'éditeur Rubrik pour mener les sauvegardes compressées, dédupliquées et chiffrées de machines virtuelles (VM) sur plusieurs sites, en Cloud privé, sur un site de PRA, chez OVH, puis Amazon Web Services au-delà d'un mois. Pour garantir les niveaux de services des VM, quatre fréquences de sauvegarde sont retenues avec leur propre règle de rétention.

« L'assurance tous risques d'une DSI, c'est d'avoir des sauvegardes fiables et performantes », souligne le manager. Son équipe IT, composée de 6 personnes pour 250 serveurs, épaule 450 salariés dans la filiale française. Dès 2009, elle met le cap sur l'industrialisation de l'infrastructure avec la virtualisation des serveurs sous VMware, puis celle des postes VDI en 2011, l'hyperconvergence avec Nutanix en 2013, la ToIP dans le Cloud en 2014, et le nouveau PRA avec Rubrik en 2017.

Olivier Bouzereau

Dossier publié dans Solutions Numériques N°20

ANNEXE 1

Présentation générale des infrastructures

1. PRESENTATION

INGEDEP est doté d'un réseau étendu de 130 sites interconnectés. On recense aujourd'hui 400 serveurs physiques et/ou virtuels au sein du Datacenter de la collectivité.
Les 47 collèges du département sont interconnectés avec le réseau d'INGEDEP et font partie des 130 sites.
On recense 2 000 postes qui se répartissent ainsi :

- 1 150 postes sur des liens haut-débit
- 650 postes sur des liaisons bas débit de type Wan connectés sur une infrastructure de postes virtuels
- 200 portables en situation de mobilité

2. ARCHITECTURE RESEAU

L'architecture réseau est organisée autour d'un cœur à 40 gigabits gérant des vlans de niveau 2 et de niveau 3 sécurisés par le protocole VRRP.
La sécurisation des équipements de distribution est réalisée grâce au protocole Spanning-Tree.
Les supports intersites sont divers : filaire, fibre optique monomode, faisceaux hertziens, liaison radio 5GHz.
Un Wan MPLS raccorde l'ensemble des sites distants du département.

2.1 Le bouclage optique

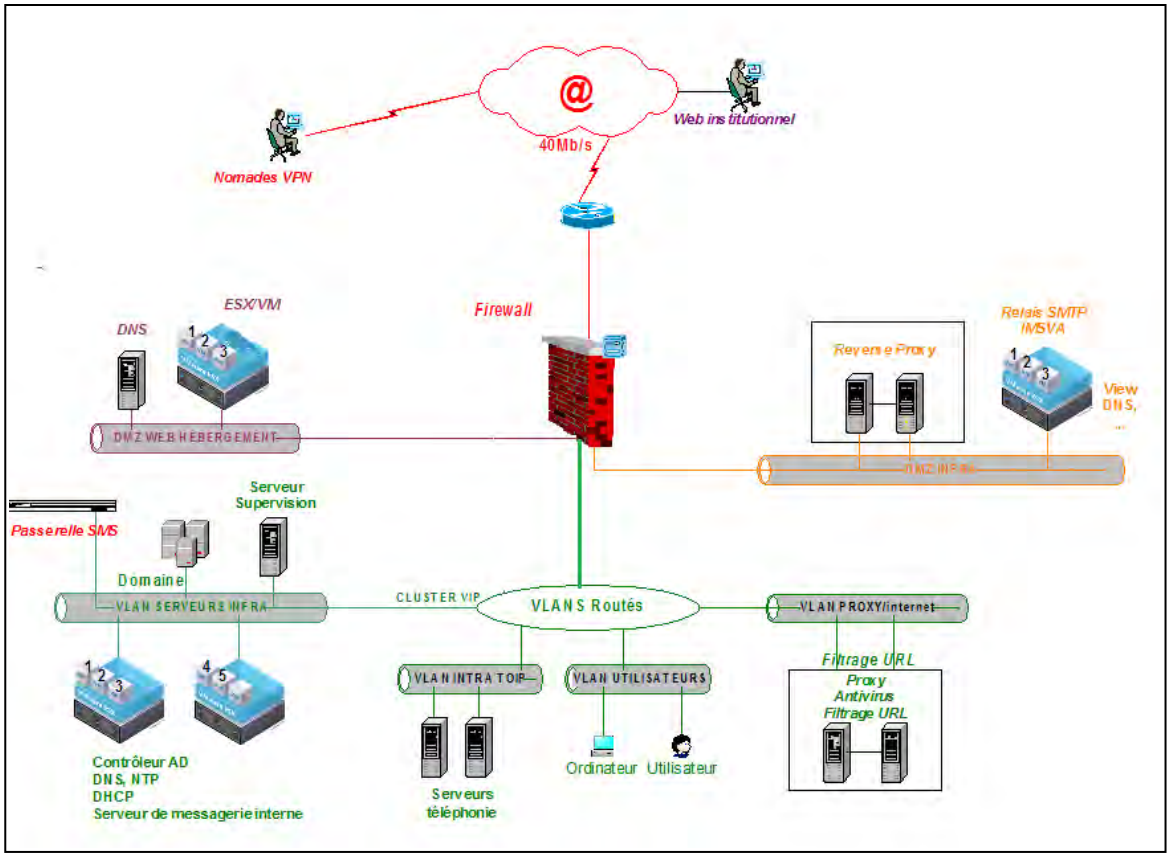
Les principaux sites métropolitains sont raccordés via une boucle optique qui permet d'assurer une sécurité accrue au niveau de l'acheminement des flux via la boucle.

2.2 Architecture WAN

L'ensemble des 130 sites « éloignés » du département d'INGEDEP sont raccordés grâce à un MPLS opérateur.
Les liens sont dimensionnés avec des liaisons SDSL de 1Mbs, 2Mbs et 4Mbs selon la taille des sites et de leur parc informatique.
Le management du réseau Wan est assuré par l'opérateur.
L'interconnexion avec le Lan est basée sur un Vlan d'interconnexion.
Lors de la perte d'un routeur, l'ensemble du trafic bascule sur le second routeur.

2.3 Architecture Internet

Un accès internet d'un débit de 40 Mb est mutualisé pour l'ensemble du personnel d'INGEDEP.
L'ensemble des éléments de l'infrastructure de sécurité : firewall, proxy, Reverse-proxy, relais de messagerie sont installés au sein du Datacenter.



2.4 Architecture Téléphonique

L'installation téléphonique d'INGEDEP est une solution constructeur et full IP dans la majorité des sites.

3. STOCKAGE

INGEDEP dispose d'une infrastructure de stockage centralisée qui intègre les technologies SAN & NAS. L'architecture actuelle est constituée de 2 baies située au sein du Datacenter.

4. ARCHITECTURE DE VIRTUALISATION

Une infrastructure de virtualisation des serveurs a été mise en œuvre sur la base de la solution VMWARE Vsphere.
Cette solution fonctionne sur une plate-forme matérielle à base de châssis de type blade et de lames à processeurs Intel, ainsi que des serveurs physiques dédiés faisant office d'hyperviseur.
Elle compte environ 400 serveurs virtuels qui reposent sur 20 serveurs physiques (ESX et ESXi).
Dans le cadre d'un PRA/PCA, une étude globale est en cours afin d'exploiter pleinement cette infrastructure de virtualisation pour un basculement rapide en cas de problème majeur au sein du Datacenter.

5. ARCHITECTURE DE MESSAGERIE

INGEDEP est équipé d'une solution de messagerie d'entreprise basée sur la solution Zimbra. Cette solution permet d'offrir les services suivants :

- Envoi / réception de messages en interne et en externe
- Messagerie en client web
- Accès à la messagerie (et agenda) pour les utilisateurs en interne et en externe pour une population d'agents (directeurs, chefs …)
- Synchronisation de la messagerie (et agenda) avec des appareils mobiles (IPhone

principalement) pour une population d'agents « VIP »

6. ARCHITECTURE DE SAUVEGARDE

L'architecture de sauvegarde d'INGEDEP est installée au sein du Datacenter et repose sur les solutions suivantes :
- l'outil de backup TINA-Time Navigator pour la sauvegarde des serveurs de fichiers
- le logiciel de sauvegarde VEAM pour la sauvegarde des environnements virtuels
- une baie disque dédiée au sein du Datacenter
- une librairie LTO6

7. SECURITE DU SYSTEME D'INFORMATION ET PROTECTION DES DONNEES

INGEDEP ne dispose pas de Politique de Sécurité du Système d'Information (PSSI).
Une charte informatique a cependant été rédigée en l'année 2002, elle est présente sur l'Intranet.
La démarche de nomination d'un Délégué à la Protection des Données (DPD/DPO) est initiée avec la Direction des Systèmes d'Information (DSI) et la Direction des Affaires Juridiques (DAF) afin d'engager les actions de conformité et notamment l'élaboration d'une démarche projet respectant les principes du RGPD.

ANNEXE 2

Rapport d'audit de sécurité du Système d'Information (SI)

Un premier audit des architectures a permis d'évaluer l'exposition du Système d'Information (SI) d'INGEDEP aux menaces externes. Il a été mené selon une approche globale composé de 3 types d'audit :

- audit macroscopique d'architecture ;
- audit macroscopique des composants antiviraux ;
- audit macroscopique des processus.

1. Audit macroscopique d'architecture

- Le composant proxy « W..... » assure la sécurité des échanges avec internet et le filtrage des URL dans le cadre de la navigation des utilisateurs ;
- La passerelle mails est équipée du logiciel « T....." » qui assurent la sécurité et le filtrage des mails échangés sur le réseau local et ceux en provenance d'internet ;
- Les postes utilisateurs sont protégés par la solution antivirale « S.....Suite » ;
- En termes de segmentation réseau, le LAN est bien découpé en VLANs mais sans étanchéité entre les segments ;
- Le routage est activé entre les VLANs, il n'existe aucune composante de type « Firewall » pour sécuriser les flux entre les différents segments ;
- En cas d'infection virale sur le VLAN utilisateurs, l'infection pourrait se propager aux infrastructures serveurs ;
- La distribution des mises à jour des systèmes d'exploitation sur les postes comme sur les serveurs n'est pas systématique. Les systèmes restent vulnérables aux attaques virales utilisant ces failles comme vecteur de propagation (faille RDP, netbios …) ;
- Certains postes connectés au SI utilisent un mode de connexion particulier (postes « NATé ») ce qui les autorise à naviguer vers l'extérieur ;
- L'architecture mise en place permet la mise à jour des composants et la récupération des dernières bases virales des postes de travail comme des serveurs ;
- L'architecture existante ne permet pas la mise en place de PCA et de PRA.

2. Audit macroscopique des composants antiviraux

- les bases virales sont mises à jour régulièrement (1 fois/jour) pour tous les composants ;
- Le composant "passerelle mails " T....." est en version X et présente un retard d'une version majeure ;
- Le rapport de protection antivirale fait apparaître 2 % des postes de travail dont le statut de protection représente un point d'attention (antivirus périmé ou désactivé).

3. Audit macroscopique des processus

- Le processus de gestion des alertes n'est pas clairement identifié et non outillé :
  - aucun document ne décrit le processus de traitement des alertes ;
  - les alertes sont reçues par mail (liste de diffusion, pas d'acteur fixe identifié pour le traitement), sans possibilité de synthèse ou de mise en avant d'évènements importants ou d'un niveau de gravité élevé ;

- les alertes ne sont pas corrélées ;
- les alertes ne donnent pas lieu à la formalisation de plans d'actions.

- Les actions et processus liés à la gestion de la plateforme antivirale mettent en évidence des problématiques de niveau de sécurité :
  - absence de comptes nominatifs, certaines tâches d'administration sont effectuées avec des comptes génériques ;
  - il est difficile d'assurer la traçabilité des actions (ajout d'exception sur la passerelle mail, ajout de règles de firewall) ;
  - les alertes ne sont pas corrélées (détection de comportement suspect par corrélation de plusieurs alertes venant de plusieurs composants), ni différenciées (analyse et classification des alertes selon leurs types/priorité) ;
  - les alertes ne donnent pas lieu à la formalisation de plans d'actions ;
  - il n'existe pas de « revue de sécurité » pour le traitement des exceptions et des demandes de modification.