CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE
DE MARTINIQUE

CONCOURS INTERNE ET TROISIEME CONCOURS DE TECHNICIEN TERRITORIAL SESSION 2014

Mercredi 19 novembre 2014

Elaboration d'un rapport technique rédigé à l'aide des éléments contenus dans un dossier portant sur la spécialité au titre de laquelle le candidat concourt.

durée : trois heures
coefficient : 1

SPECIALITE : INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION

A LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET

Ce dossier comporte 30 pages, y compris celle-ci.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

- ✓ Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou nom fictif, ni votre numéro de convocation, ni signature ou paraphe.
- ✓ Aucune référence (nom de collectivité, nom de personne, ...) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.
- ✓ Seul l'usage d'un stylo à encre soit noire, soit bleue est autorisé (bille non effaçable, plume ou feutre). L'utilisation d'une autre couleur pour écrire ou souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
- ✓ Les feuilles de brouillon ne seront en aucun cas prises en compte.

Le non respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

Technicien au sein du service informatique de la ville de Techniville (55 000 habitants), on vous a récemment demandé de travailler sur la mise en oeuvre d'un télé service pour les demandes d'état civil.
Un logiciel a été acquis, fonctionnant en mode SaaS (Software as a Service), et la mise en oeuvre est pratiquement terminée. Ce logiciel est qualifié comme « produit de confiance » par l'organisme habilité (ANSII). Il s'agit maintenant de s'assurer de la mise en conformité globale de ce télé service, au regard du RGS (Référentiel Général de Sécurité).
Un premier audit des scénarios de menaces pouvant porter sur le système a été réalisé par un prestataire externe. Cet audit n'incluait pas la formalisation d'un plan d'action visant à répondre aux menaces identifiées.

Le directeur des systèmes d'information vous demande de rédiger à son attention, exclusivement à l'aide des documents ci-joints, un rapport technique sur la mise en conformité au RGS.

Liste des documents joints :

Document 1 : « Les données informatiques ne sont pas assez protégées » www.lagazettedescommunes.com – 2013 – (2 pages)

Document 2 : « Etude EBIOS ville du Havre » - Société Demaeter, www.demaeter.fr Février 2012 - (1 page)

Document 3 : « Comment contacter mon observatoire zonal de la SSI » - Agence Nationale de la Sécurité des Systèmes d'Information, www.ssi.gouv.fr Décembre 2013 (2 pages)

Document 4 : « EBIOS : la méthode de gestion des risques SSI, un outil simple et puissant » - Agence Nationale de la Sécurité des Systèmes d'Information (ANSII), www.ssi.gouv.fr/ebios - Avril 2010 - (2 pages)

Document 5 : « La lettre sécurité Solucom » – Solucom, www.solucom.fr - Septembre 2010 (3 pages)

Document 6 : « Extrait du RGS » - Agence Nationale de la Sécurité des Systèmes d'Information (ANSII), www.ssi.gouv.fr - Mai 2010 - (2 pages)

Document 7 : « RGS » - Université du sud Toulon Var, Twardy, cesar.resinfo.org Juin 2013 - (11 pages)

Document 8 : « Rapport d'audit des scénarios de menaces portant sur la mise en oeuvre du télé services à la mairie de X » wwww.ssi.gouv.fr - 2010 - (1 page)

Document 9 : « Une stratégie de sécurité informatique complète et cohérente doit inclure le contrôle des utilisateurs à privilèges », Solution Wallix, www.wallix.com - juin 2013 – (2 pages)

Document 10 : « Organisation de la sécurité » - ssi-conseil, www.ssi-conseil.com Novembre 2005 - (2 pages)

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

DOCUMENT 01

la gazette.fr

CYBERSÉCURITÉ

« Les données informatiques des collectivités locales ne sont pas assez protégées »

E. Lesquel | France | Publié le 28/01/2013

Dans un entretien accordé à La Gazette lundi 28 janvier 2013, lors du 5e forum international de la cybersécurité, le commandant Rémy Février, chargé de mission intelligence économique à l'état-major de la région de gendarmerie Nord-Pas Calais pointe du doigt la vulnérabilité des systèmes d'information des collectivités.

Rémy Février est ancien cadre du secteur privé et un ancien dirigeant d'un cabinet de consulting en stratégie. Il est désormais officier professeur sous contrat à la gendarmerie nationale.
Il enseigne l'intelligence économique et territoriale en masters spécialisés à l'école nationale d'administration, en écoles supérieures de commerce et à l'université. Il est également un ancien élu d'une ville de plus de 100 000 habitants.

En matière de cybersécurité, les collectivités sont-elles assez protégées ?

Non, mais il existe très peu données concrètes et aucune étude au niveau national. De plus, les collectivités sont réticentes à parler des problèmes rencontrés.
Cependant, à la vue de mon expérience de terrain et du sondage que j'ai pu réaliser auprès d'une soixantaine de collectivités du Nord-Pas de Calais dans le cadre de ma thèse, les lacunes des collectivités et en particuliers des communes dans ce domaine sont énormes. Ces résultats sont transposables à l'ensemble du territoire.

Pourquoi les communes sont-elles les plus vulnérables ?

C'est l'échelon territorial qui détient le plus de données sensibles et c'est aussi souvent là que les moyens pour se protéger sont les plus faibles. Pourtant, que ce soit la prise de contrôle à distance d'un poste de travail, la modification de documents sensibles, l'usurpation d'identité, ou tout simplement la perte de données, la menace est réelle. En cas de problèmes, la responsabilité des élus est clairement engagée.

Un élu peut se retrouver mis en examen pour avoir insuffisamment protégé ses systèmes d'informations ?

Tout à fait. Même si la réglementation dans ce domaine est jurisprudentielle, il ressort clairement qu'un élu, au même titre qu'un chef d'entreprise, peut être mis en examen pour ne pas avoir pris les mesures nécessaires pour se protéger. Or, 70 % des collectivités interrogées ne connaissent pas les responsabilités qui leur incombent !

Les collectivités sont-elles vraiment menacées ?

Avec le développement de l'e-democratie, de l'e-administration, ou de la dématérialisation des appels d'offres, le risque est réel. Il n'y a pas de raisons que les attaques que le secteur privé subit tous les jours ne soient pas transposées dans le secteur public.
Qu'est ce qui empêchera demain une entreprise d'aller voir l'offre faite pas ses concurrents dans le cadre d'un appel d'offre ? Qui pourra empêcher une personne mal intentionnée de diffuser des informations confidentielles collectées illégalement auprès d'une collectivité ?

Quels sont les points à améliorer d'urgence ?

Il s'agit avant tout de créer une culture de la sécurité des systèmes d'information à tous les niveaux et donc de former tout le personnel. Pour cela, les élus doivent être moteurs.
Dans un premier temps, des choses très simples peuvent êtres mises en œuvre comme, ne pas laisser le mot de passe sur un post-it sur l'écran du PC ou ne pas se débarrasser de ses anciens ordinateurs sans s'être au préalable assuré qu'il n'y ait plus de données dessus !

Le niveau des protections est-il vraiment si faible ?

Malheureusement oui. Plus de 65 % des collectivités interrogées n'ont pas de responsable informatique et les trois quarts n'ont pas de budget dédié à la sécurité de leurs systèmes d'information. Sans parler de malveillance, la simple sécurisation des données est déjà très problématique. Plus de 60 % des collectivités interrogées ne les externalisent pas. En cas d'incendie ou d'inondations, elles peuvent alors tout perdre et ne plus êtres capables de fonctionner correctement.

Que faut-il mettre en place pour sauvegarder efficacement des données ?

Il faut absolument qu'elles soient sauvegardées sur deux lieux différents, et pas simplement deux pièces d'une mairie ! Par exemple, il s'agit de déposer régulièrement ces données à la banque ou de faire appel à un prestataire extérieur. Dans ce cas, il s'agit de bien s'assurer de la fiabilité de ce prestataire. Par exemple, vérifier qu'il ne stockera pas les informations dans le cloud, qui n'est pas forcément le lieu le plus sécurisé !

Et pour se prémunir des attaques existe-t-il une recette ?

Du bons sens avant tout. 80 % des problèmes sont évitables avec de simples mesures de bon sens. Pour aider les collectivités à mieux se protéger, l'Etat a publié un très bon référentiel général de sécurité des systèmes d'informations [1].
Malheureusement, il ressort du sondage que les trois quarts des collectivités ne connaissent pas ce document et qu'à même proportion elles ne connaissent pas jusqu'à l'existence de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) qui est pourtant l'agence de référence. C'est toute une nouvelle culture qu'il faut aujourd'hui créer autour de ces nouveaux risques.

DOCUMENT 02

demæter
tout se transforme

LE HAVRE

Client	**Ville du Havre**
Résumé	**Étude EBIOS du Guichet Unique de Gestion de la Relation Citoyen**

Contexte et enjeux du client

Le rôle du Guichet de la Relation Citoyen (GRC) est de fédérer au sein d'un guichet unique, sous une même authentification et une même norme graphique et de navigation, un ensemble de services offerts par divers acteurs (ville, communauté d'agglomérations, syndicat des transports, syndicat des eaux...).
S'agissant d'un téléservice de l'administration, la conformité au RGS est un impératif.
Par ailleurs, la Ville du Havre, au-delà de l'obligation de conformité, souhaitait ne prendre aucun risque sur la sécurité des données personnelles des citoyens.

Les enjeux de la Ville du Havre étaient les suivants :

- Conformité RGS du Guichet Unique de la Relation Citoyen
- Sécurité des données personnelles des citoyens
- Sécurité juridique de la solution

Période d'intervention

Février 2012

Contribution de DEMAETER

- Étude de sécurité
- Recommandations d'amélioration de la sécurité

Bénéfices pour le client

- Plan d'action d'amélioration de la sécurité
- Conformité RGS

Environnement technique

- Solution de dématérialisation YPOK

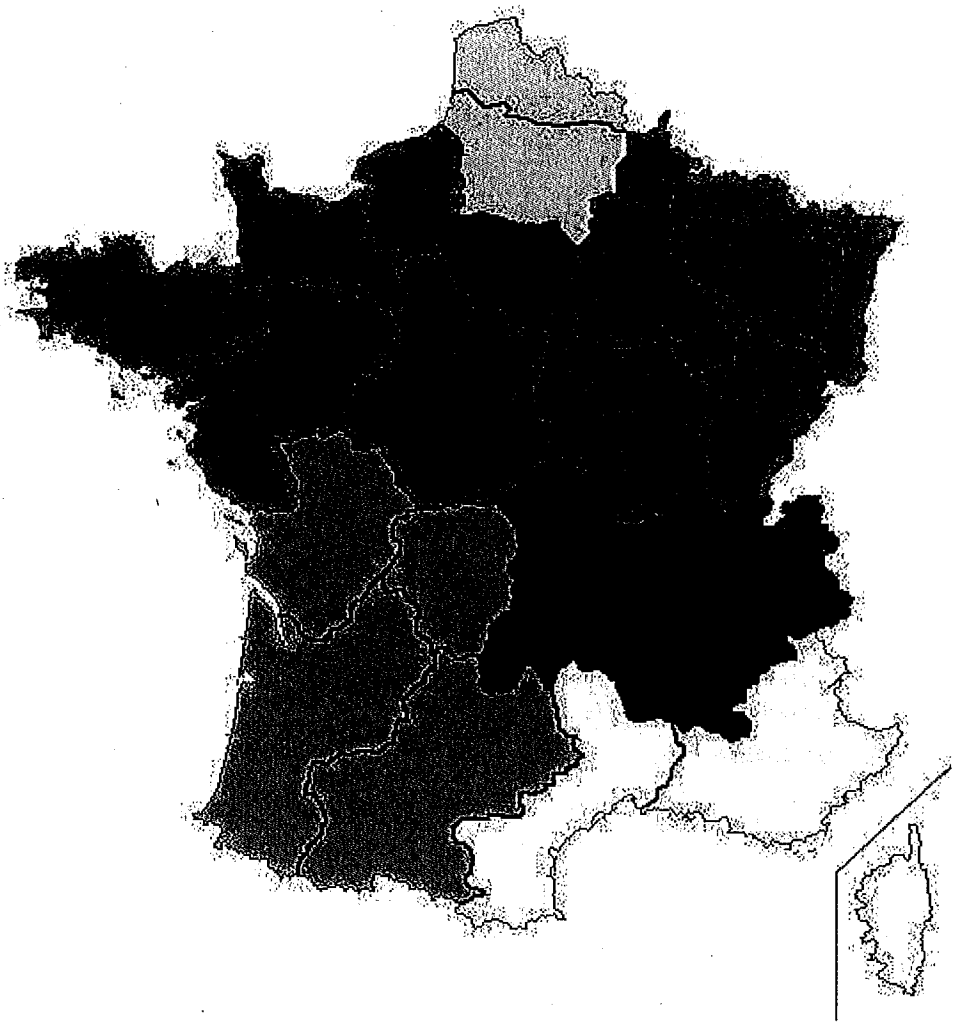
Contact

- **Jean-Luc Thorel** (DSI)

DOCUMENT 03

Comment contacter mon observatoire zonal de la SSI ?

Cliquez sur la carte ci-dessous pour accéder aux coordonnées de votre observatoire zonal de rattachement.



Source iconographique : Wikipedia

Pourquoi s'appellent-ils des observatoires ?

Historiquement, le concept des OzSSI a été défini suite à une initiative locale dans la zone de défense Est. Cette initiative a fait que l'observatoire zonal de la SSI de la zone de défense Est existe maintenant depuis plusieurs années. Pour faciliter la mise en place des OzSSI dans les autres zones de défense, ce terme d'"observatoire" a donc été conservé pour permettre de se référer facilement à l'exemple de la zone de défense Est.

Qu'observent les OzSSI ?

Les OzSSI doivent contribuer à relayer l'action de l'Etat depuis l'échelon central, l'ANSSI, vers tous les échelons locaux. À ce titre, ils doivent observer si les aides et les moyens mis en place au niveau central contribuent à satisfaire les besoins au niveau local. Les OzSSI ne sont pas une entité hiérarchique ou une autorité zonale, ils servent de relais territorial de l'action de l'Etat dans le domaine de la SSI et disposent à ce titre de moyens de communication privilégiés avec l'ANSSI.

Quel est le rôle du délégué ?

Dans chaque zone de défense, un délégué est désigné pour animer l'OzSSI local. Il est rattaché au préfet délégué pour la sécurité et la défense, qui est chargé d'assister le préfet de zone pour toutes les missions concourant à la sécurité publique, à la sécurité civile et à la défense à caractère non militaire.

Le délégué de l'OzSSI a pour mission d'animer un réseau de partage d'expérience entre tous les acteurs SSI locaux.

Quel est le périmètre d'action des OzSSI ?

Les observatoires sont mis en place au profit de tous les acteurs locaux ayant des besoins en matière de sécurité des systèmes d'information :

- échelons déconcentrés de l'Etat,
- collectivités territoriales (mairies, conseils régionaux et généraux),
- organismes ayant une mission de service public (hopitaux, syndicats des eaux, etc.),
- opérateurs d'importance vitale,
- organismes "métiers" (chambres de commerce et d'industrie, chambres des notaires, conseils de l'ordre, etc.),
- entreprises sensibles.

Suis-je obligé d'adhérer ?

La participation au réseau d'entraide suppose une démarche volontaire des adhérents. Cette démarche est aussi garante de l'instauration d'un climat de confiance entre les participants. L'OzSSI n'est ni un lieu d'inquisition, ni un lieu de délation. Il doit permettre de faciliter les échanges entre des responsables ayant des préoccupations similaires.

Quelles informations m'apportent les OzSSI par rapport à la consultation des sites de l'ANSSI ?

L'une des mission des OzSSI est de faire connaître les différentes ressources mises en place par l'ANSSI pour aider la société de l'information à prendre en compte la sécurité des systèmes d'information (site institutionnel, portail de la sécurité informatique, flux RSS, autoformations, etc.).

Mais les OzSSI sont le relais territorial de l'ANSSI. À ce titre, ils disposent de moyens de communication privilégiés avec l'ANSSI, notamment d'un accès à un extranet sécurisé où sont disponibles des informations de veille en matière de SSI.

Que m'apportent les OzSSI par rapport à ma chaîne fonctionnelle SSI ?

Les OzSSI sont mis en place en priorité pour tous ceux qui ne bénéficient pas du soutien d'une chaîne fonctionnelle SSI. Toutefois, ils doivent permettre de mieux connaître le tissu local des acteurs de la SSI et de partager les expériences.

Ils sont également chargés d'organiser localement des séances thématiques regroupant leurs adhérents autour d'un même besoin (sensibilisation, formation, sujet technique, etc.)

Dois-je remonter mes incidents aux OzSSI ?

Ce n'est en aucun cas une obligation. Les règles de chaque entité en matière de SSI doivent toujours être respectées et la remontée d'incident suivre la voie fonctionnelle SSI mise en place. Si cette voie fonctionnelle n'existe pas, les incidents peuvent être remontés directement au CERTA.

Mais les délégués des OzSSI disposent de moyens de communication privilégiés avec l'ANSSI. Ils constituent son relais territorial et peuvent donc vous aider à remonter des informations sensibles en toute confidentialité.

Quel est le rôle du ministère de l'intérieur dans la mise en place des OzSSI ?

La direction de la planification de sécurité nationale (DPSN) a pour mission l'élaboration des instructions en vue de l'application territoriale des plans gouvernementaux et le suivi de leur mise en œuvre. C'est au titre de cette mission interministérielle territoriale que la mise en place des OzSSI s'est effectuée grâce aux moyens du ministère de l'intérieur.

Quel est le rôle des OzSSI dans la réorganisation territoriale de l'État ?

Les OzSSI n'ont pas de mission particulière au titre de la réorganisation territoriale de l'État. Les responsables SSI de cette réorganisation, qui devraient être désignés au niveau départemental, ont toutefois vocation à participer aux travaux des OzSSI de leur zone de défense. Là encore, cela permettra de faciliter les échanges de bonnes pratiques

ANSSI | Agence nationale de la sécurité des systèmes d'information

EBIOS : la méthode de gestion des risques SSI
Un outil simple et puissant

La gestion des risques est largement décrite et préconisée dans la presse, les normes, la réglementation... EBIOS® (Expression des Besoins et Identification des Objectifs de Sécurité) est la méthode de gestion des risques de l'ANSSI. Opérationnelle, modulaire et alignée avec les normes, c'est la boîte à outils indispensable pour toute réflexion de sécurité des systèmes d'information (SSI). Voici comment EBIOS peut vous être utile.

Le risque SSI dans EBIOS : un exemple éclairant

Définition du risque : c'est un scénario qui combine un événement redouté (sources de menaces, bien essentiel, critère de sécurité, besoin de sécurité, impacts) et un ou plusieurs scénarios de menaces (sources de menaces, bien support, critère de sécurité, menaces, vulnérabilités).

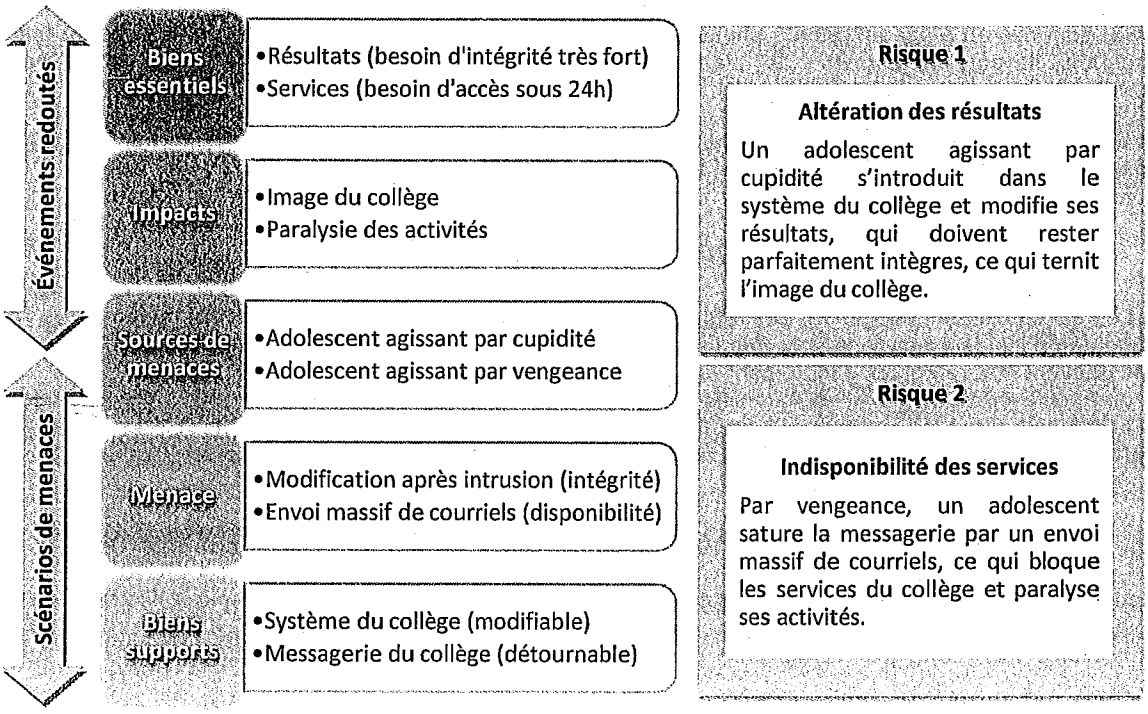
On estime son niveau par sa gravité (hauteur des impacts) et sa vraisemblance (possibilité qu'il se réalise).

Un adolescent de 15 ans « pirate » le système informatique de son collège pour améliorer ses notes.

Un adolescent de quinze ans a en effet été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.

[Sources Internet : Le Point.fr et ZDNet]

À partir de ce fait divers et de la définition du risque d'EBIOS, nous pouvons mettre deux risques en évidence :

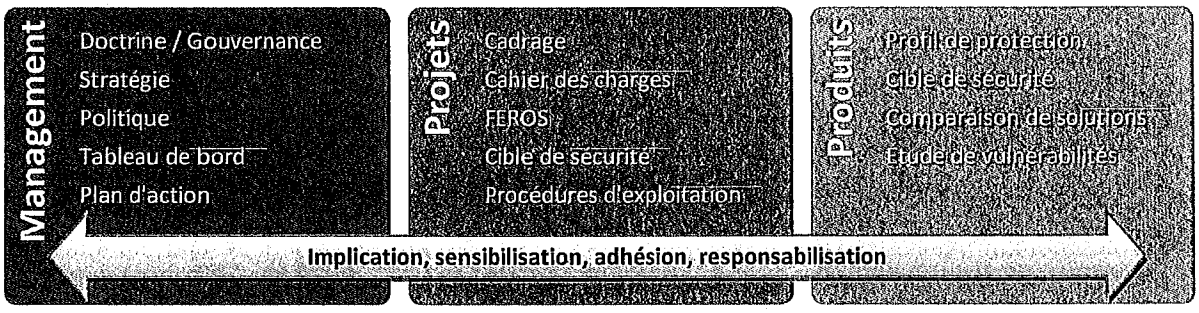


Une étude EBIOS appliquée au système du collège aurait permis, simplement et rapidement :

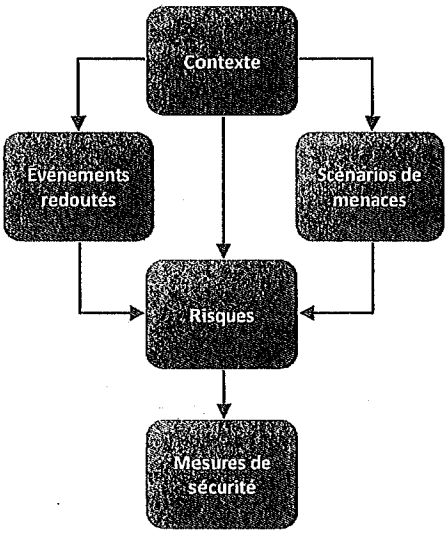
- d'identifier ces deux risques, ainsi que tous les autres qui pèsent sur le système d'information du collège ;
- d'estimer leur niveau (gravité, vraisemblance), les cartographier et prendre des décisions en conséquence ;
- de choisir les mesures nécessaires et suffisantes en termes de prévention, de protection et de récupération.

ANSSI | Agence nationale de la sécurité des systèmes d'information

EBIOS est le "tout terrain" pour gérer les risques



Les 10 questions essentielles pour gérer les risques



Contexte	•Pourquoi et comment va-t-on gérer les risques ? •Quel est le sujet de l'étude ?
Événements redoutés	•Quels sont tous les événements craints ? •Quels seraient les plus graves ?
Scénarios de menaces	•Quels sont tous les scénarios possibles ? •Quels sont les plus vraisemblables ?
Risques	•Quelle est la cartographie des risques ? •Comment choisit-on de les traiter ?
Mesures de sécurité	•Quelles mesures devrait-on appliquer ? •Les risques résiduels sont-ils acceptables ?

Grands principes à appliquer

Pour réussir une étude et son application, il convient de respecter 4 grands principes de mise en œuvre :

- employer EBIOS comme une boîte à outils pour une efficacité maximale ;
- utiliser la méthode avec souplesse pour adhérer au langage et aux pratiques de l'organisme ;
- améliorer progressivement l'étude, en temps réel, pour rester cohérent avec la réalité ;
- rechercher une adhésion des acteurs du système d'information pour élaborer des solutions de protection.

Une mise en œuvre facilitée

La méthode dispose de bases de connaissances riches et enrichissables, d'un logiciel libre et gratuit, de formations et d'une documentation variée.

La communauté des experts et utilisateurs de gestion des risques (industriels, administrations, prestataires, universitaires...) se réunit régulièrement au Club EBIOS pour échanger des expériences et enrichir le référentiel.

EBIOS ne vous protège pas des risques, elle vous permet d'en faire prendre conscience aux décideurs.

Informations : http://www.ssi.gouv.fr/ebios
Contact : ebios@ssi.gouv.fr

n° 22 - Septembre 2010

La Lettre Sécurité

Trois sujets au programme de cette lettre. Tout d'abord un dossier sur le référentiel général de sécurité (RGS). L'Agence nationale de sécurité des systèmes d'information (ANSSI) l'a publié en mai 2010. Patrick Pailloux, son Directeur général, a bien voulu répondre à nos questions sur ce référentiel et je l'en remercie. Deux sujets d'actualité ensuite : d'une part, la sécurité des *smartphones* et les nouvelles stratégies pour les intégrer au SI en maîtrisant ses risques ; d'autre part, les nouvelles réglementations en matière de sécurité pour les opérateurs de jeux en ligne.

Je profite de cette lettre pour vous rappeler que comme tous les ans, Solucom sera présent aux *Assises de la Sécurité* à Monaco du 6 au 9 octobre 2010. Nous y animerons cette année un atelier sur les 15 dernières années de la sécurité... et les perspectives pour les années à venir, au travers d'une table ronde qui réunira Gil DELILLE (RSSI du Crédit Agricole), Thierry OLIVIER (RSSI de SFR) et Sylvain THIRY (RSSI de la SNCF).

Je vous invite tous à y participer et à venir nous rencontrer sur notre stand.

Bonne lecture à tous !

Frédéric GOUX
Directeur
practice Sécurité & risk management

Dossier

Le référentiel général de sécurité : applicable à l'administration, utile pour tous

Le développement de l'administration électronique est l'un des fers de lance de la politique de modernisation de l'État. De nombreuses administrations ont mis en place des services en ligne à destination de leurs usagers (impôts, changement d'adresse, casier judiciaire, emploi, paiement des amendes...) ou des entreprises (téléTVA, déclarations sociales, compte fiscal...) La sécurité de ces services en ligne est un élément fondamental pour garantir la confiance des utilisateurs. C'est pour répondre à cet enjeu qu'a été élaboré le référentiel général de sécurité (RGS).

Périmètre et objectifs du RGS

Le référentiel général de sécurité (RGS) a été officiellement approuvé par arrêté du Premier Ministre le 6 mai 2010. Ce texte, résultat d'un travail conjoint entre l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Direction générale de la modernisation de l'État (DGME) a pour objectif de **développer la confiance des usagers et des administrations dans leurs échanges numériques.**

Le RGS vise à améliorer le niveau de sécurité de toute autorité administrative mettant en œuvre des systèmes d'information susceptibles d'échanger des informations avec des usagers ou avec d'autres autorités administratives.

Par « autorité administrative » on entend les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant les régimes de protection sociale et les organismes chargés de la gestion d'un service public administratif.

Le RGS concerne aussi l'ensemble des éditeurs de produits et prestataires de services de confiance (PSCO) souhaitant voir leurs produits ou services être qualifiés et être ainsi choisis par les autorités administratives voulant sécuriser leurs téléservices.

Contenu du RGS

La première partie du RGS pose **un cadre général pour gérer la sécurité des systèmes d'information** au sein des autorités administratives. Ce cadre s'appuie sur les bonnes pratiques du marché en matière de sécurité (ISO 27001, ISO 27005) et sur les documents de référence publiés par l'ANSSI (méthode EBIOS d'analyse de risques, guide de maturité SSI, PSSI type, guide d'intégration de la sécurité dans les projets...).

Le RGS édicte **six grands principes** en matière de sécurité des systèmes d'information (voir encart page 2). S'imposent notamment :

• La mise en place d'une approche de la sécurité « pilotée par les risques ». Il s'agit

solucom
management & IT consulting

notamment de **conduire systématiquement une analyse de risques** lors de la conception ou de l'évolution d'un système d'information, afin d'identifier en amont les mesures de sécurité à implémenter par rapport aux enjeux et aux besoins de sécurité.

• **L'homologation de sécurité** d'un système d'information préalablement à sa mise en service opérationnelle. Cette homologation, à conduire par une « autorité d'homologation » habituellement au sein de l'autorité administrative, permet de vérifier que le système d'information est protégé conformément aux objectifs de sécurité fixés suite à l'analyse de risques. Cette homologation doit être motivée et justifiée, généralement par l'analyse d'un dossier de sécurité. Dans le cas d'un téléservice, l'attestation d'homologation doit être rendue accessible aux usagers.

• Le recours, chaque fois que possible, à des **produits de sécurité** et **des prestataires de services de confiance labellisés** pour leur sécurité. Le processus de labellisation (« qualification ») des produits et prestataires de services est piloté par l'ANSSI.

Six grands principes de gestion de la SSI

1. Adopter une démarche globale
2. Adapter la SSI selon les enjeux
3. Gérer les risques SSI
4. Élaborer une politique SSI
5. Utiliser les produits et prestataires labellisés pour leur sécurité
6. Viser une amélioration continue

La suite du RGS fournit des **règles de sécurité plus précises** pour plusieurs fonctions de sécurité. La version en vigueur du RGS (version 1.0 du 6 mai 2010) couvre les **fonctions d'authentification, de signature électronique, de confidentialité et d'horodatage.** Pour chacune de ces fonctions, les règles fournies par le RGS sont différenciées selon plusieurs niveaux de sécurité (*, **, ***) qui permettent d'adapter les mesures de sécurité aux enjeux et aux besoins spécifiques de chaque système d'information. La version 1.0 du RGS a repris les documents qui constituaient l'ancienne PRIS (Politique de référencement intersectoriel de sécurité) dans sa version 2.3.

Il est intéressant de noter que le RGS déconseille – sans pour autant la bannir – l'utilisation d'un simple couple « identifiant / mot de passe » pour assurer la fonction d'authentification.

Le RGS introduit par ailleurs de nouvelles exigences, relatives à :

• La fourniture d'un **accusé de réception élec-**

Témoignage

Patrick PAILLOUX

Directeur général de l'Agence nationale pour la sécurité des SI (ANSSI, www.ssi.gouv.fr)

Qu'est ce qui a motivé la mise en place du RGS ?

Devant l'essor des téléservices, il paraissait naturel que l'État se dote des règles permettant de garantir la sécurité de ses systèmes d'information, au-delà du périmètre des informations classifiées dont la protection était encadrée depuis de nombreuses années.

L'objectif du RGS est de définir un texte à portée générale, applicable par l'ensemble des autorités administratives, quels que soient leur taille et leurs enjeux. En effet, le RGS doit permettre à la fois de sécuriser le site internet d'une petite mairie, tout comme des systèmes d'information très complexes et à forts enjeux tels que les déclarations fiscales des entreprises et des particuliers.

L'élaboration du RGS a-t-elle été complexe ?

La validation d'un tel texte nécessite de suivre un parcours assez chronophage : consultation publique, notification à la Commission européenne, avis de la Commission consultative d'évaluation des normes (CCEN), etc.

Au-delà de ce premier point, la principale complexité a été de parvenir à un texte apportant des réponses concrètes en matière de sécurisation des systèmes d'information, tout en restant suffisamment général pour s'adapter à tous les types d'entités concernés.

Comment évaluez-vous la maturité actuelle des autorités administratives par rapport à ce texte ?

La maturité est évidemment très inégale, mais les enjeux et les risques sont très variés selon les autorités administratives. Le RGS permet justement d'aider les autorités administratives à positionner le juste niveau d'exigence en matière de sécurisation. Pour des systèmes d'information à forts enjeux, les mesures de sécurité à implémenter seront relativement poussées. Pour les systèmes à enjeux moindres, il ne faut pas se faire une montagne du RGS : on se contentera d'actions élémentaires de sécurisation, telles que la mise en place d'une politique de mots de passe, le déploiement de correctifs de sécurité, etc.

tronique et, le cas échéant, d'un accusé d'enregistrement électronique pour toute demande, déclaration ou production de documents adressée par un usager à une autorité administrative par voie électronique.

• **La validation par l'ANSSI** des certificats électroniques utilisés dans le cadre de services en ligne. Cette validation est fondée sur l'analyse d'un dossier de « demande de validation », éventuellement complétée par la réalisation d'audits sur place.

Calendrier de mise en œuvre du RGS

Le calendrier de mise en œuvre du RGS vise une mise en conformité de l'ensemble des systèmes d'information concernés d'ici à mai 2013 :

• Les systèmes d'information existant à la date de publication du RGS doivent être mis en conformité dans un délai de **trois ans** (échéance : mai 2013).

• Les systèmes d'information créés dans les six mois qui suivent la publication du RGS doivent être mis en conformité dans un délai de **12 mois** (échéance : fin 2011).

Analyse

Le référentiel général de sécurité apporte enfin un cadre général, complet et pérenne en matière de sécurité des SI, obligatoire pour toutes les autorités administratives françaises et recommandé plus largement pour l'ensemble des entreprises françaises. Il constitue de ce fait un réel outil à la disposition du RSSI pour légitimer sa démarche et améliorer au fil du temps le niveau de sécurité de son organisation.

Pour autant, même s'il amène quelques exigences nouvelles, le RGS n'est pas une révolution : il s'appuie en particulier sur les normes internationales et les publications de l'ANSSI qui guident les actions des RSSI depuis de nombreuses années ; il laisse par ailleurs la latitude et la responsabilité à chaque entité de choisir le niveau de sécurité à implémenter en fonction de ses enjeux et de ses risques.

D'un point de vue technique, le RGS augmente le niveau d'exigences minimales requises, notamment en ce qui concerne les infrastructures cryptographiques (tailles de clés, algorithmes utilisés...).

De nombreuses autorités administratives ont déjà lancé des actions d'alignement avec le RGS. Tout laisse à penser que ce dernier deviendra rapidement le livre de chevet de beaucoup de RSSI, y compris en dehors de l'administration !

Guillaume DURAND

En savoir plus : www.ssi.gouv.fr/rgs

Quel est le rôle de l'ANSSI vis-à-vis du RGS ?

L'ANSSI a pour mission d'assister les autorités administratives dans la mise en œuvre du RGS. L'ANSSI veille par ailleurs à faire évoluer le RGS dans le temps, en l'enrichissant de nouveaux contenus et en apportant les ajustements qui s'avéreront nécessaires. L'objectif est de maintenir au fil du temps un référentiel complet et à jour, en intégrant des guides et des recommandations sur des sujets spécifiques. Nous travaillons par exemple actuellement sur les problématiques de sécurité dans l'externalisation des SI.

Des actions de contrôle, voire des sanctions en cas de non-conformité, sont-elles prévues ?

Le RGS a été conçu pour aider les autorités administratives dans l'amélioration progressive de leur niveau de sécurité. Les exigences du RGS seront naturellement intégrées dans le cadre des inspections SSI réalisées par l'Agence, mais clairement l'objectif de ce texte n'est pas de sanctionner.

Le RGS préconise le recours à des produits et à des prestataires labellisés pour leur sécurité. Des actions sont-elles prévues pour enrichir ce référentiel ?

Concernant les produits de sécurité, l'ANSSI a créé récemment le label CSPN (certification de sécurité de premier niveau) qui permet de labelliser un produit au terme d'une expertise moins formelle que celle des Critères Communs. La charge pour obtenir un label CSPN est de 25 à 35 hommes/jour. Depuis août 2008, 11 certificats sur 23 demandes ont déjà été accordés, soit environ 50% de réussite. D'ailleurs la plupart des candidats qui échouent représentent leur produit, qu'ils ont renforcé grâce au rapport de certification. D'autres opérations de certification sont actuellement en cours.

L'ANSSI a également mis en place un circuit de labellisation des prestataires de services « qualification ». En version 1.0 du RGS, deux familles de prestataires peuvent être qualifiées : les prestataires de services de certification électronique et les prestataires de services d'horodatage. Des travaux sont en cours sur les prestations d'archivage électronique et les prestations d'audit et de test d'intrusion.

Les initiatives actuelles autour d'une identité numérique « fédérée » vont-elles dans le sens du RGS ?

Le RGS pose une trajectoire visant à augmenter le niveau de sécurité de nos systèmes d'information ; nous sommes bien entendu très favorables à toutes les initiatives allant dans ce sens. C'est notamment le cas de projets tels que le label IDéNum ou le projet de carte nationale d'identité électronique (CNIE).

Quels sont les autres grands sujets d'actualité pour l'ANSSI, un an après sa création ?

L'activité de l'agence est forte, avec notamment la mise en place du centre opérationnel de détection des attaques informatiques, des actions sur la résilience des infrastructures vitales de la France (notamment les infrastructures télécoms), la mise en place de produits pour garantir un haut niveau de sécurité aux télécommunications de l'administration, des actions de communication plus régulières, etc. L'effectif de l'Agence est d'environ 150 personnes aujourd'hui ; nous prévoyons d'être 250 en 2012 : le recrutement et l'intégration des nouveaux embauchés fait aussi partie des challenges de l'ANSSI dans les années à venir !

Propos recueillis par Frédéric GOUX et Guillaume DURAND

2.3 - Intégration de la SSI dans le cycle de vie des systèmes d'information

Dans tout projet de mise en place d'un système d'information, le besoin de sécurité doit être pris en compte avec la même attention, en même temps et au même titre que les besoins fonctionnels que vise à satisfaire le système, le téléservice ou l'application.

Prise très en amont du projet, son efficacité sera bien supérieure, et son coût bien moindre, que s'il faut faire évoluer les spécifications, voire les équipements ou l'architecture du système, du fait d'une intégration tardive. Il est ainsi recommandé de considérer la SSI dès la phase de définition du système d'information (voire même dès l'étude d'opportunité en cas de doute sur la possibilité de sécuriser le système d'information au niveau requis), puis au-delà, tout au long de sa vie, notamment lors de toute modification, jusqu'à son retrait du service. Cette démarche de réévaluation et d'amélioration constante de la SSI s'appuie notamment sur des audits réguliers de sécurité. En fin de vie, il convient, par exemple, de veiller à la destruction des données et des composants confidentiels, avant de céder, de jeter ou de détruire le système.

Dans ce cycle, une étape essentielle est l'homologation de sécurité du système d'information (§ 2.3.2), qui doit intervenir avant la mise en service du système, puis être régulièrement réexaminée, afin de prendre les mesures que peuvent imposer les évolutions du système, de ses composants, de son emploi, du contexte humain ou organisationnel, ou encore bien sûr de la menace.

2.3.1 - Des efforts proportionnés aux enjeux SSI

La démarche de sécurité doit être adaptée aux enjeux du projet. Dans ce but, il est recommandé d'utiliser le guide [GISSIP] de l'ANSSI pour l'intégration de la sécurité dans les différentes phases des projets informatiques, et en particulier :

- lors de la conception générale, pour identifier les objectifs généraux de sécurité ;
- lors de la conception détaillée, pour affiner les objectifs de sécurité et identifier le niveau de risque maximum que l'autorité responsable se déclare prête à accepter ;
- lors de la réalisation du système, pour décrire concrètement les mesures de sécurité et la manière de les appliquer dans l'environnement effectif d'utilisation ;
- à la fin de la phase de développement et au plus tard avant la phase d'exploitation, pour prononcer la décision d'homologation (§2.3.2) ;
- tout au long de la vie du système, jusqu'au retrait du service, pour maintenir la sécurité.

2.3.2 - Un engagement systématique : l'homologation de sécurité

> Extrait du [DécretRGS] : Chapitre II : Fonctions de sécurité des systèmes d'information :
> Article 5 :
> L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 3.
> Dans le cas d'un téléservice, cette attestation est rendue accessible aux usagers selon les mêmes modalités que celles prévues à l'article 4 de l'ordonnance du 8 décembre 2005 susvisée pour la décision de création du téléservice.»

Cette « attestation formelle », évoquée à l'article 5 *supra,* correspond à une « homologation de sécurité du système d'information ». Celle-ci est obligatoire et est un préalable à la mise en service opérationnelle de tout système d'information. Elle est prononcée par une autorité dite d'homologation, désignée par l'AA, habituellement au sein même de cette AA. Lorsque le système est sous la responsabilité de plusieurs AA, l'autorité d'homologation est désignée conjointement par les AA concernées.

Au sens de l'article 5 *supra*, la décision d'homologation, ou « attestation formelle », est l'engagement par lequel l'autorité d'homologation atteste, au nom de l'AA, que le projet a bien pris en compte les contraintes opérationnelles de sécurité établies au départ, que les exigences de sécurité sont bien déterminées et satisfaites, que les risques résiduels sont maîtrisés et acceptés, et que le système d'information est donc apte à entrer en service.

Afin que sa décision soit motivée et justifiée, il est recommandé que l'autorité d'homologation s'appuie sur un dossier de sécurité, constitué selon le modèle décrit dans le guide [GISSIP].

Selon les résultats de l'analyse effectuée lors de la démarche d'homologation, l'autorité d'homologation pourra prononcer :

- une homologation provisoire, assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ;
- une homologation, assortie le cas échéant de conditions, pour une durée déterminée (recommandée entre 3 et 5 ans) ;
- un refus d'homologation, si les résultats de l'audit font apparaître des risques résiduels jugés inacceptables.

2.3.3 - Des outils spécifiques pour différentes familles de téléservices

Il est recommandé que les experts SSI et les responsables de système d'information utilisent, pour exprimer les besoins de sécurité et identifier les objectifs de sécurité, des fiches d'expression rationnelle d'objectifs de sécurité (FEROS). Pour faciliter ce travail, et pour les familles les plus usuelles de téléservices qu'une AA peut mettre en œuvre, sept FEROS génériques [FEROSTypes] sont proposées :

- Téléservice de candidature (exemples : candidature dans l'enseignement supérieur, au permis de conduire, ...) ;
- Téléservice de consultation (exemples : consultation des remboursements de la sécurité sociale, des résultats d'examens, de concours, ...) ;
- Téléservice de déclaration (exemples : dossier fiscal du particulier (TéléIR), compte fiscal des professionnels, déclaration de changement d'adresse, ...) ;
- Téléservice de demande (exemples : demande d'extraits d'état civil, de permis de construire, de licence IV, de stage d'étudiants, ...) ;
- Téléservice d'inscription (exemple : inscription à un concours de la fonction publique) ;
- Téléservice de paiement en ligne (exemples : paiement d'amendes, règlement de la TVA, règlement d'impôts sur le revenu, ...) ;
- Téléservice de simulation (exemples : calcul de revalorisation des pensions alimentaires, simulateur de calcul de retraite, d'impôt sur le revenu, ...).

En complément, le guide d'exigences de sécurité [ExigencesTélé] propose un ensemble d'exigences de sécurité qui permettent de répondre aux objectifs de sécurité exprimés dans les [FEROSTypes].

Il est recommandé de s'appuyer sur ces documents chaque fois que le téléservice mis en place entre dans l'une des familles présentées *supra*.

Le cadre juridique

- Prévu par l'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
  - élaboré conjointement par l'ANSSI et la DGME
- Le décret n°2010-112 du 2 février 2010 fixe ses conditions d'élaboration, d'approbation, de modification et de publication.
- Le 18 Mai 2010 est publié au journal officiel l'arrêté du Premier ministre du 6 Mai 2010 portant approbation du RGS.
- Le RGS est aujourd'hui en cours d'évolution, le RGS V2 disponible sur le site de l'ANSSI est actuellement en phase d'appel à commentaire.

A qui s'adresse le RGS ?

- Sont concernés par le RGS les autorités administratives mettant en œuvre des télé-services à destination de ses usagers ou d'autres autorités administratives (AA).
- Il s'adresse tout particulièrement aux :
  - RSSI, DSI, chefs de projets MOA-MOE, etc.
  - Prestataires de services fournissant des certificats et aux constructeurs de produit de sécurité.

Autorité Administrative ?

- L'ordonnance 2005-1516 du 8 décembre 2005
  - «Article 1 Sont considérés comme autorités administratives au sens de la présente ordonnance les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif.».
- Les universités sont des établissements publics à caractère scientifique, culturel et professionnel sous-ensemble des établissements publics à caractère administratif.

Qu'est ce que le RGS ?

- Il n'impose ni technologie ni solution technique, sa seule exigence est l'homologation de sécurité du télé-service basé sur un dossier de sécurité résultant d'une analyse de risques, et ce avant sa mise en production.
- Il présente un ensemble de recommandations et de bonnes pratiques en matière de SSI basées sur une amélioration continue et une approche globale de la SSI.
- Il défini des règles concrètes que doivent respecter les fonctions de sécurité relatives à l'authentification, la signature électronique, la confidentialité et l'horodatage.

Démarche de mise en conformité RGS

- s'inscrit dans une démarche globale de gestion des risques SI tout au long du cycle de vie du télé-service
- Le RGS défini 5 étapes à respecter :
  - Réalisation d'une analyse de risque (ISO27005/EBIOS)
  - Définition des objectifs de sécurité (FEROS)
  - Choix et mise en œuvre des mesures de sécurité en termes de protection et de défense (rgs, norme Iso 27002, guide d'exigences de sécurité des télé-procédures type, PSSI, catalogue interne de mesures applicables, guide de développement, etc.)
  - L'homologation de sécurité
  - Suivi opérationnel de la sécurité

L'homologation de sécurité

- Elle doit être prononcée par une autorité d'homologation sur la base d'un dossier de sécurité conforme au modèle décrit dans le GISSIP, réalisé par une commission d'homologation.
- Par cette homologation l'AA atteste :
  - que le projet a bien pris en compte les aspects de sécurité dès la phase d'étude d'opportunité,
  - qu'il a fait l'objet d'une étude de risque et qu'il est apte à traiter les informations au niveau des besoins de sécurité exprimés,
  - que les objectifs de sécurité définis lors de l'étude sont atteints,
  - que les risques résiduels sont acceptés et maitrisés.
- Elle peut être provisoire, refusée ou accordée pour une durée déterminée (entre 3 et 5 ans)

Recommandations et bonnes pratiques

10

- Veille documentaire
- Adopter une démarche globale résultant d'une volonté cohérente et globale, il est recommandé de :
  - Considérer tous les aspects, techniques et non techniques
  - Prendre en compte la SSI au juste niveau hiérarchique
  - Responsabiliser tous les acteurs
  - D'intégrer la SSI tout au long du cycle de vie des SI.
- Adapter la Sécurité des SI selon les enjeux et les besoins de sécurité, d'y consacrer les moyens financiers et humains justes nécessaires et suffisants. (guide de maturité SSI, GISSIP)
- Impliquer les instances décisionnelles
- Organiser la Sécurité des Systèmes d'Information
- Organiser les responsabilités liées à la SSI

Recommandations et bonnes pratiques

- Mettre en place un SMSI dans le but d'une amélioration continue de la SSI. (Iso 27001)
- Elaborer une PSSI
- Sensibiliser le personnel aux bonnes pratiques en matière de sécurité
- Utiliser les produits et prestataires labellisés pour leur sécurité
- Mettre en place des mécanismes de défense des systèmes d'information
- Procéder à des audits réguliers de la sécurité du système d'information
- Elaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité

Recommandations et bonnes pratiques

- Prendre en compte la sécurité dans les contrats et les achats
- Prendre en compte la sécurité dans les projets d'externalisation et de cloud-computing
- Réaliser une veille sur les menaces et les vulnérabilités
- Utilisation des catalogues de mesures de sécurité relatives à la sécurité des systèmes d'information
- Favoriser l'interopérabilité notamment au travers du respect du Référentiel Général d'Interopérabilité (RGI).

Pour résumer : Etre conforme RGS c'est

- Avoir mené une analyse de risque afin :
  - d'identifier les biens à protéger
  - d'identifier les menaces pouvant avoir un impact
  - de hiérarchiser les risques
  - de déterminer les objectifs de sécurité en termes de disponibilité, confidentialité, intégrité, traçabilité afin de réduire les risques
  - de déterminer les fonctions et mesures de sécurités à mettre en œuvre.
- De respecter le cas échéant les règles décrites dans le RGS pour les fonctions d'authentification, signature, confidentialité, horodatage au niveau déterminé.
- D'utiliser des produits qualifiés par l'ANSSI
- D'attester par l'homologation de sécurité la prise en compte de la sécurité tout au long du cycle de vie de l'application
- De publier l'homologation sur le site web de l'institution

Dossier de sécurité minimal

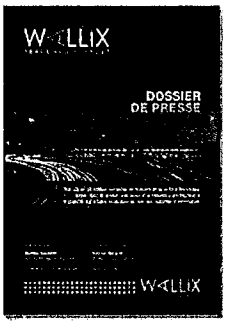
17

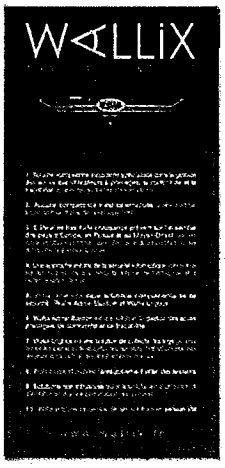
- Le cahier des charges SSI contenant à minima :
  - La définition des responsabilités concernant le télé-service
  - La description du télé-service
  - Les contraintes légales et réglementaires pesant sur le télé-service
  - Les risques hiérarchisés
  - Les objectifs de sécurité (MOA)
  - Les exigences minimales à respecter (MOE)
  - La liste des objectifs de sécurité couverts par les exigences minimales et les objectifs de sécurité non couvert.
- Les documents d'exploitation du télé-service (liste de mesures appliquées afin de répondre aux objectifs de sécurité et aux exigences minimales, éventuellement les indicateurs permettant de s'assurer de l'efficience des mesures, liste des actions par acteurs à mener au quotidien pour s'assurer de la bonne marche du télé-service, la procédure de revue des droits d'accès au télé-service.)

DOCUMENT 08

Rapport d'audit sur les scénarios de menaces portant sur la mise en œuvre du télé service à la mairie de X

Scénarios de menaces	Sources de menaces	Probabilité
Réseau interne		
Menaces sur le réseau causant une indisponibilité	Employé peu sérieux Maintenance informatique Virus Piratage Incendie des locaux Panne électrique Phénomène naturel (foudre, usure, ...)	3. Forte
Menaces sur le réseau interne causant une altération	Employé peu sérieux Maintenance informatique Virus Piratage	2. Significative
Menaces sur le réseau interne causant une compromission	Employé peu sérieux Maintenance informatique Piratage	2. Significative
Réseau Wifi		
Menaces sur le réseau Wifi causant une indisponibilité	Employé peu sérieux Maintenance informatique Virus Incendie des locaux Panne électrique Phénomène naturel (foudre, usure, ...)	3. Forte
Menaces sur le réseau Wifi causant une altération	Employé peu sérieux Maintenance informatique Virus	3. Forte
Menaces sur le réseau Wifi causant une compromission	Employé peu sérieux Maintenance informatique	3. Forte
Système de l'hébergeur		
Menaces sur le système de l'hébergeur causant une indisponibilité	Hébergeur Virus Panne électrique Phénomène naturel (foudre, usure, ...)	4. Maximale
Menaces sur le système de l'hébergeur causant une altération	Hébergeur Virus Piratage	3. Forte
Menaces sur système de l'hébergeur causant une compromission	Hébergeur Concurrent Piratage	4. Maximale





AgenceMCC.com
Relations Publiques
Relations Presse
Communication d'Entreprise
01 42 78 95 88

Jean-Noël de Galzain : «Une stratégie de sécurité informatique complète et cohérente doit inclure le contrôle des utilisateurs à privilèges»

Paris, le 11/06/2013 - Ces dernières années, cyberdéfense et cybersécurité ont pris une place considérable dans la vie des entreprises et des particuliers. Les jours passent et les attaques s'amplifient. Elles sont toujours plus ciblées, diversifiées et étendues, et la cybercriminalité fait partie intégrante de notre vie quotidienne.

Historiquement, les éditeurs d'antivirus et de pare-feu ont pris le leadership du marché. Paradoxalement, ils ne traitent qu'une partie des problèmes ce qui se traduit par une augmentation du nombre d'incidents et de leur ampleur, malgré la croissance des budgets de sécurité informatique. En effet, un pan entier de la sécurité informatique reste méconnu : la gestion des utilisateurs à privilèges, qui répond au nom encore mal connu en France, d'Insider Threat ou gestion de la menace interne.

Pour l'éditeur français, WALLIX, spécialiste de la traçabilité des utilisateurs à privilèges, une stratégie de sécurité complète et cohérente doit, certes, prévoir de se protéger contre les menaces provenant de l'extérieur mais également des risques qu'impliquent la liberté absolue dont jouissent les utilisateurs à privilèges.

Un utilisateur à privilège, qu'est-ce que c'est ?

Un utilisateur à privilège, est, par définition, une personne dont les droits ont été élevés ou étendus sur le réseau informatique : droits d'accès, gestion des autorisations, administration des équipements et applications, modification, suppression ou transfert de fichiers, etc. L'utilisateur à privilèges peut être interne ou externe à une société. Ses droits lui sont délégués par le représentant légal de la société qui souvent n'est même pas au courant de ce risque. Par nature, l'utilisateur à privilèges a donc accès à des données sensibles et stratégiques pour l'entreprise aux secrets de l'entreprise et de ses salariés. Il a un droit de vie et de mort sur l'informatique de l'entreprise.

L'utilisateur à privilèges fait-il toujours partie d'une société ?

Lorsqu'une société externalise la gestion d'une partie ou de l'ensemble de son informatique ou de ses équipements, les prestataires qui prennent la main à distance ou interviennent sur le réseau interne pour mener à bien des opérations de support ou de maintenance deviennent des utilisateurs à privilèges, et ce, bien qu'ils ne fassent pas partie des effectifs de la société. Savez-vous par exemple quelles sont les autorisations d'accès d'un technicien qui vient réparer la photocopieuse IP ou la connexion réseau ?

En d'autres termes, externaliser revient, pour une entreprise et son dirigeant, à confier « les clés de la maison » à une personne inconnue, qui aurait accès à l'ensemble des pièces et du contenu des placards, avec la capacité de les fouiller, d'y prendre et remettre ce qu'il y trouve, en gérant lui-même les autorisations d'accès. Si quelque chose est endommagé, disparaît ou est simplement dérobé après son passage, que faire ? Comment savoir ce qui a été fait ? Où y a-t-il eu un problème ? Quand ? De quelle manière ? Qui va payer les dégâts ? Comment vais-je pouvoir justifier l'incident ou le vol vis-à-vis des assurances ?

Pour le Clusif et son panorama 2012 des menaces informatiques, près de la moitié des entreprises de plus de 200 salariés en France, et des collectivités territoriales externalisent la gestion de leur Système d'information, 50% ne collectent pas les logs (pas de preuve), 20% ne changent jamais les mots de passe y compris lorsqu'un départ ou un changement de prestataire survient.

Quels sont les risques liés aux utilisateurs à privilèges ?

De par leur statut, les utilisateurs à privilèges, au même titre que les utilisateurs « lambda » font peser des risques sur le réseau d'entreprises. On peut les classer en plusieurs catégories :

Les risques liés à l'erreur humaine : comme n'importe quel utilisateur, l'utilisateur à privilèges reste un être humain, susceptible pour quelque raison que ce soit de commettre des erreurs sur un réseau ; seulement ces erreurs peuvent avoir des conséquences considérables sur la productivité, la réputation et le chiffre d'affaires de l'entreprise affectée.

Imaginons, par exemple, qu'après une erreur de manipulation lors d'une opération de télémaintenance, un prestataire externe provoque une panne sur le serveur d'un e-commerçant. Pour ce dernier, ce sont des pertes de chiffre d'affaires pendant toute la durée de la panne qu'il est nécessaire de réparer, mais avant cela d'en retrouver l'origine. Ceci peut prendre un temps considérable, multiplier les dégâts mais également entacher sérieusement la réputation de l'e-commerçant définitivement. Entretemps, les clients iront se servir ailleurs.

Désormais, avec les nouvelles réglementations, il sera nécessaire de communiquer sur un incident, avec un risque d'amende liée à la perte d'informations clients (données clients, numéros de carte bleue, ou encore, données de santé).

Dans un autre cas récent, des centaines de dossiers patients se sont retrouvés publiés sur Internet. C'est en tapant son nom par hasard dans un moteur de recherche qu'une personne a retrouvé l'intégralité de son dossier médical en libre consultation. Ce type

de fuite de données peut provenir d'une erreur humaine (un prestataire externe commet une faute dans les process et laisse s'échapper ces données) ou d'un acte de malveillance qui illustre les risques liés aux utilisateurs à privilèges.

Les risques liés à la malveillance : l'utilisateur à privilèges reste un être humain. Ainsi, lorsqu'une collaboration professionnelle se finit en mauvais termes, il peut être tentant d'utiliser ses droits pour nuire à l'entreprise ou voler des informations stratégiques (fichiers clients, CB, secrets, ...).

En 2012, c'est un sous-traitant de la société Toyota qui, après avoir été licencié, avait dérobé des informations relatives aux brevets industriels du constructeur japonais. Combien de bases clients dérobées, de messages divulgués ou d'informations recueillies grâce à des fichiers informatiques indûment téléchargés ? Là encore, se pose la problématique de l'origine de la fuite. Qui a fait cela ? Quand et comment ? Pourquoi cette personne a-t-elle eu accès à ces données en particulier ? Peut-on empêcher un tel acte ou en garder la trace et comment ? Comment gérer cela en interne et avec les prestataires externes ?

Selon une étude Forrester, 50 % des utilisateurs à privilèges partent de leur entreprise ou sortent d'une mission d'infogérance avec des données sensibles. Comment peut-on donc évaluer ou mieux encore parler de gestion des risques sans traiter ce sujet ? Quand les hautes autorités de sécurité nationale mettront elles en garde contre ces risques béants ?

Heureusement, de plus en plus de DSI et de RSSI, pour répondre au contrôle interne ou à leurs directions générales, prévoient l'usage d'une solution qui réponde au problème de la gestion de la menace interne et des prestataires externes. Aussi ont-ils prévu l'intégration d'une solution de gestion des utilisateurs à privilèges dans leurs politiques de sécurité.

Le marché français du PUM (Privileged User Management) n'en est qu'à ses balbutiements malgré l'urgence.

WALLIX, éditeur pionnier dans la gestion des utilisateurs à privilèges grâce à sa solution Wallix AdminBastion, le WAB, préconise, bien entendu la protection contre les menaces provenant de l'extérieur du réseau. Elles sont connues et désormais très bien circonscrites grâce à des solutions comme l'anti-virus, le firewall, l'IPS, l'IDS etc. Cependant, l'éditeur français insiste sur la nécessité et l'urgence de compléter ces dispositifs par des solutions internes de contrôle des utilisateurs à privilèges.

Cependant, ces solutions souffrent d'une mauvaise réputation : trop souvent, celles-ci sont perçues comme des produits visant purement et simplement à surveiller les utilisateurs à privilèges. Contre toute attente, elles permettent surtout de dédouaner les utilisateurs en apportant une preuve tangible et concrète de l'origine de l'incident.

Pour Jean-Noël de Galzain, fondateur de WALLIX, l'éditeur pionnier de solution de gestion des utilisateurs à privilèges, le WAB : *« une stratégie de sécurité cohérente de bout-en-bout ne peut plus se passer de solutions de contrôle des utilisateurs à privilèges. Chaque jour, des utilisateurs à privilèges accèdent à des données essentielles et stratégiques pour la survie et la rentabilité de l'entreprise. Même si, bien entendu, la malveillance n'est généralement pas la première cause de perte de données, les erreurs humaines sur un réseau, sont, elles, bien réelles et peuvent prendre des proportions catastrophiques à l'échelle de l'Internet. Nous alertons vivement les DSI, RSSI et les plus hautes instances de sécurité informatiques quant aux risques qui pèsent en termes de productivité, de réputation et de conformité sur les entreprises publiques et privées. La gestion des risques internes est aussi prioritaire que la gestion des menaces périmétriques. Le risque le plus grave serait de l'ignorer ! »*

WALLIX est pionnier dans la sécurisation des accès informatiques et la traçabilité. Ainsi Wallix AdminBastion est une solution de traçabilité et de contrôle des utilisateurs à privilèges. En agissant comme un SAS d'authentification pour l'ensemble des utilisateurs à privilèges, Wallix AdminBastion permet de tracer leurs actions, de les visualiser ultérieurement. Ainsi, la recherche de l'origine d'un incident est facilitée. En aidant à la recherche de preuve Wallix AdminBastion permet également aux entreprises de renforcer leur conformité (compliance) aux normes de sécurité informatique en vigueur, telles que PCI DSS, SOX, Bâle II, etc. La solution Wallix AdminBastion est simple d'utilisation et sans agent. Elle se déploie en quelques heures dans le SI et permet de contrôler l'ensemble des activités des comptes à privilèges.

Jean-Noël de Galzain, PDG de WALLIX

DOCUMENT 10

ORGANISATION DE LA SÉCURITÉ

14-11-2005

L'organisation de la sécurité doit rester en adéquation avec les moyens de l'entreprise et la structure pouvant être mise en place dans une grande entreprise, éventuellement organisée sur plusieurs pays, n'aura rien à voir avec celle d'une Petite voire Moyenne Entreprise.
Cependant, il faut se rappeler que les risques sont indépendants de la taille de l'entreprise et dès lors qu'il peut s'agir de sa survie, ils sont, toutes proportions gardées, plus élevés pour une PME du fait justement de la limitation des moyens pouvant être investis en sécurité. Les PME conscientes de ce paradoxe se tourneront avantageusement vers des solutions de sécurité mutualisées, sous-traitées ou hébergées.

Principes d'organisation :

L'organisation de la sécurité dans l'entreprise doit **respecter la règle de la séparation des rôles** entre :

- **La responsabilité de la sécurité :** Maîtrise d'ouvrage confiée au RSSI, responsable de la sécurité des informations devant la Direction Générale;
- **La responsabilité de la réalisation de la politique de sécurité :** Maîtrise d'œuvre souvent confiée à la DSI ou Direction de Systèmes d'Information, responsable de la mise en œuvre des solutions de sécurité inscrites dans le schéma directeur sécurité,
- **Le contrôle de la sécurité :** l'Audit ou le Contrôleur indépendant, il est chargé de mener des missions d'audit et de contrôle de l'efficacité et du respect de la politique de sécurité de l'entreprise.

Acteurs et Missions de l'organisation de la sécurité :

Le RSSI : Responsable de la sécurité des informations et du système d'information, il 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 est rattaché au meilleur niveau hiérarchique possible dans l'entreprise et dispose d'un budget spécifique. **En vertu des principes évoqués plus haut, il n'est pas sous la responsabilité du DSI.** Son action transverse à toutes les organisations de l'entreprise dont l'informatique exigent de lui un certain nombre de savoir-faire et de savoir-être :

- excellente connaissance de l'analyse et du traitement des risques, capable de gérer un référentiel des actifs et d'en faire approuver la classification en sensibilité (criticité) par les métier selon une approche par les processus,
- bonne connaissance des métiers de l'entreprise et une curiosité permanente compte-tenu de ses missions de veille technologique,
- capable de mettre en place avec les métiers des contrôles dont les indicateurs seront remontés directement à la Direction Générale (sans intermédiaires) en vue d'un pilotage effectif des risques d'entreprise,
- compétences techniques permettant un dialogue avec les spécialistes, notamment système et réseaux de l'informatique,
- des compétences d'organisateur car il est responsable de la mise en place du schéma directeur de la sécurité dont certains aspects comme les plans de reprise d'activité sont complexes,
- des compétences de communication pour faire face à ses missions de sensibilisation,
- des compétences de négociateur, de diplomatie et de management compte-tenu de l'étendue du domaine dans lequel il évolue et de l'aspect transverse de sa mission.

"Au-delà de son excellence technique, le RSSI doit être un professionnel de la communication pour mobiliser son DG ", commente Pascal Antonini, associé Ernst & Young.
Ressources :
on trouvera une excellente définition des rôles et fonctions du RSSI dans le document : Risk Manager et RSSI : document PDF de 1Mo & 64 pages réalisé par l'AMRAE (Association pour le management des risques et des assurances de l'entreprise) et le CLUSIF (Club de la sécurité de l'information Français).
Un RSSI banque s'exprime suite à l'affaire de la Société Générale : Les Nouvelles du Net :Sécurité et Contrôle dans les Banques : un echec ?

Le Comité Sécurité :

Il est composé d'un responsable de la sécurité informatique (**RSI**) et d'un responsable sécurité métiers auprès des utilisateurs (**RSU**) . Animé par le RSSI, il permet de mieux partager les implications de la mise en œuvre de la politique de sécurité entre les deux pôles. Il met au point la réalisation du schéma directeur, décide des priorités, des actions en cours ou des réactions aux incidents de sécurité. Il est responsable de l'organisation des plans de secours.

L'équipe sécurité :

Rassemblant des spécialistes système et réseaux formés aux problématiques de sécurité, elle assure la mise en œuvre technique de la sécurité du système d'information.
Lorsque c'est possible, il est intéressant de développer au sein de l'entreprise une entité permanente ou cellule de veille conforme au modèle du CERT afin de disposer de spécialistes capables d'apporter une réponse rapide suite à la découverte d'une intrusion ou d'une faille de sécurité.

Le Contrôle de la sécurité :

Il s'exerce a trois niveaux :

- le contrôle utilisateur : il s'agit de l'implication des utilisateurs et de leur hiérarchie pour s'assurer du respect de la politique de sécurité;
- L' audit interne : il peut être diligenté par les services d'audits internes ou d'audits informatiques,
- L'audit externe : réalisé par une entité indépendante comme un cabinet spécialisé.

Cellules de veille, cellules de crise : se reporter au chapitre continuité d'activité.

Le RPCA : Responsable du Plan de Continuité des Activités Métiers :
Le responsable du plan de continuité des activités métiers prépare avec les utilisateurs l'ensemble des dispositions nécessaires pour assurer la reprise des activités de chaque service critique en cas de sinistre majeur.
Il prévoit : Cellule de crise, moyens logistiques et de transports, lieux et moyens matériels de reprise d'activité, plan de retour à la normale en connexion avec le plan de reprise des activités informatiques.
Il assure par des exercices (pas toujours faciles à organiser) le maintien en conditions opérationnelles de ce plan.

Dernière mise à jour : (18-03-2009)