11. janvier 2018 16:56:04
GENERAL.CARTAU.SSI.Cours.2018-01-05a.odt

SÉCURITÉ DES SYSTÈMES D'INFORMATIONS - COURS

Cédric Cartau

Principe de Sutton
Si vous avez une idée, sachez que quelqu'un l'a déjà eu avant vous.
Même cette idée je l'ai piquée à quelqu'un d'autre.

Généralités
Écriture d'une note sur le SI
Écriture d'une note sur la SSI

Le gâteau de grand-mère
- écriture de requête SQL
- déployer un AV sur un parc de 100 PC ou 100 000 PC
- permettre l'accès au DPI de 1000 patients ou 3M de patients

Note sur une prise de décision technique
Appréciation des risques dans une DRH
Appréciation des risques dans une conception de datacenter
Appréciation des risques dans une conception de campus (double DC, plusieurs bâtiments, adductions Voix et IP, etc.)

Éléments de stratégie
Exercice de maturité selon Doc28 et Doc29
Exercice de maturité COBIT sur un déploiement AV

Le SMSI

Les autres projets
Conception d'une infra PCA-PRA
Conception d'une infra IAM
Réflexion sur les problèmes d'architecture et de processus de sauvegarde
Conception d'une infra BLAC
Conception d'une sécurisation de parc, incluant le Wifi
Réflexion sur une infra de traçabilité
Réflexion sur une politique d'audit
- Concevoir un audit technique
- Concevoir un audit orga
- Concevoir un plan d'audit
Réflexion sur l'archivage
Conception d'une infra AV
Conception d'un réseau sécurisé
Réflexion sur la conformité
Réflexion sur la protection Cloud

Table des matières

1. Introduction

1.1. Présentation de l'intervenant

1.2. Histoire raccourcie de la SSI

La sécurité SI vue sous l'angle réseau
Les piles de protocoles
Les VLAN
Les Firewall, filtrages d'URL, VPN

La sécurité sous l'angle système
Sécurisation des OS
Sécurisation des middleware
Sécurisation des comptes de connexion
Problématique récente induite par la virtualisation

2. Généralités

1er janvier 2028 : les systèmes Cobol corrigés pour ne pas planter le 1er janvier 2000... plantent.
1er janvier 2031 : les processus automatiques des serveurs HP-UX 10 s'arrêtent subitement.
1er janvier 2037 : WindowsNT 4.0 et les programmes écrits en Visual C++ 4 plantent.
19 janvier 2038 : les Unix 32 bits et les programmes en C sont datés au 1er janvier 1970. Les processus automatiques des serveurs HP-UX 11 s'arrêtent.
31 décembre 2040 : l'horloge des mainframes IBM s'arrête à minuit et le système cesse de prendre en compte les dates.

8 juin 2046 et 1er juillet 2048 :
les mots de passe Unix ne sont plus reconnus... deux fois de suite.
1er janvier 2068 : les serveurs sous Solaris et Linux pensent être revenus au 1erjanvier 2000.
10mai 2071 :les IBMAS/400 pensent être revenus au 23 août 1928.
1er mars 2100: plantage probable de plusieurs systèmes qui pensaient en toute logique être le 29 février, alors que cette année-là n'est pas bissextile

2.1. Définitions

SI
SSI

2.2. Les fondamentaux managériaux

2.2.1. Prise de décision en environnement à haute technicité

Théorie des décisions absurdes

2.2.2. La différence entre le gâteau de mamie et la cuisine du self

Notion d'industrialisation
Rajouter exemples de requêtes SQL
Maturité dev
Maturité conception / réalisation / sécurité

2.2.3. Principes de contrôle des organisations modernes

3 principes généraux
Organisations structurées, pyramidale, transversales ou matricielle
Séparation de l'expertise et de la décision
Séparation de l'action et du contrôle

Séparation de l'action et du contrôle
Base de tout le système Qualité
Application générale du principe de la roue de Déming (PDCA)
Fondement de toutes les normes ISO

2.2.4. Déplacement du centre de gravité

Années 50 : production industrielle
Années 60 et 70 : technologie
Années 80 et 90 : finances (chute d'Enron en 2001)
Années 2000 : qualité et audit

Exemple : la gestion des admin système
Application du PDCA
Lien avec la certification des comptes, impacts sur le projet IAM et les habilitations métier

Exemples techniques
La protection AV

L'analyse des traces du BLAC

Réponse à l'objection du temps passé à rédiger des procédures
Exemple de l'aviation civile
Typologie des incidents IT
Le premier bug : entre la chaise et le clavier...de l'informaticien

2.3. Les fondamentaux de la SSI

2.3.1. Les 4 axes

Axes de la sécurité :
- disponibilité ;
- confidentialité ;
- intégrité ;
- dans un second temps, preuve et contrôle ;

Exemple de disponibilité : application de conduite d'une chaîne de production de véhicule.
Exemple de confidentialité : gestion de la médecine du travail dans un CH/CHU.
Exemple d'intégrité : application d'archivage de données notariales, application de dossier patient, etc.
Exemple de preuve / dépôt : application de dépôt / retrait d'un Appel d'Offre.

2.3.2. Le cas particulier du D

Notion de RTO et RPO

2.3.3. Schéma conceptuel général d'appréciation du risque

Articulation entre :
- menace (+ probabilité d'occurrence) ;
- vulnérabilité (+ facilité d'exploitation) ;
- actif (besoin en DICP) ;
- risque
- impact (sur une matrice d'impacts) ;

LA SECURISATION EST LA REPONSE A L'IMPACT D'UN RISQUE

2.3.4. Le traitement du risque

Réduction, transfert, évitement, acceptation

Exemple :
- identification d'un risque de disponibilité sur la messagerie (par exemple serveur non doublé) ;
- 4 stratégies : acceptation, évitement (plus de messagerie !), réduction (2nd serveur) ou transfert (externalisation de la messagerie) ;
- choix par un décideur de la stratégie à adopter au regard de la stratégie générale de l'entreprise ;

De la limite de la réduction du risque

2.3.5. Approche managériale du risque

Arbitrage entre le coût de réduction et le coût d'acceptation

Exemple du juridique

2.4. Approche Qualité versus approche technique

2.4.1. L'approche Qualité

Principe général de gestion de la Qualité dans les organisations modernes : celui qui fait <> celui qui ordonne <> celui qui contrôle

Deux paradigmes : l'ingénierie et la qualité
Ingénieur = faire, bien tout de suite, et passer au dossier / problème suivant
Qualité = faire, pas forcément parfaitement tout de suite, mais s'améliorer tout le temps

Je suis né à Sioux City, petite ville du centre des Etats-Unis, le 14 octobre 1900.
Je suis mort le 20 décembre 1993.
Je suis diplômé de l'Université de Yale.
Ma spécialité est la physique théorique.
Durant ma carrière, j'ai été statisticien, professeur, auteur, conférencier et consultant.
J'ai inventé la roue
Je suis….
Je suis….
Je suis…

William Edwards Deming

Notion de PDCA

2.5. Notion de niveau de maturité

Les trois stades de réalisation

Les concepts COBIT

Exemple de l'échelle COBIT
Niveau 0, inexistant : l'entreprise n'est pas consciente du besoin
Niveau 1, initial : l'entreprise est consciente du besoin mais rien n'existe pour le satisfaire

Niveau 2, répétitif mais intuitif : traitement au cas par cas, en s'appuyant sur la connaissance de quelques individus
Niveau 3, défini : procéduré et formalisé, mais responsabilités individuelles ; il n'existe aucun reporting formel ni aucun suivi de la qualité
Niveau 4, géré et mesurable : les responsabilités sont claires, la qualité est suivie, les personnels formés et les outils automatisés
Niveau 5 : veille afin de mettre à jour les méthodes et se tenir à l'état de l'art

Application de l'échelle COBIT à la protection AV

Extrait DSIH, juin 2016, voir Annexe 4

2.6. Aspects juridiques et normatifs

Les normes et certifications :
- HAS ;
- contraintes normatives de certains secteurs : ISO 15189
- CICF ;

Les lois
- loi du 4 mars 2002
- loi de santé 2015
- Décret hébergeur ;
- prochaines évolutions de la réglementation CNIL : obligation de déclaration des incidents de sécurité, règlement européen ;
- PSSI nationales et sectorielles

2.7. Les fondamentaux techniques

Le chiffrement
Les mots de passe

2.8. Conclusion

La sécurité SI doit être prise en compte en amont dans tous les projets
La sécurité SI n'est pas un logiciel ou un matériel, mais une démarche transversale
La sécurité SI comporte la notion de procédures dégradées, qui sont de la responsabilité des MOA
La sécurité SI doit impliquer fortement les directions MOA
La sécurité SI n'est pas une fin en soit, mais un arbitrage entre des contraintes (production, fonctionnalités, coûts, etc.)
La sécurité SI n'apporte aucun bénéfice directement démontrable…tant qu'il n'y a pas de sinistre

2.8.1. Exemples de la vie courante

Les appareils photos numériques (intégrité)
La gestion des comptes bancaires sur Internet (confidentialité)
L'accès Internet (disponibilité)

Le quadriptyque DICA
Exemple de progiciel à contraintes de disponibilité
Exemple de progiciel à contraintes d'intégrité

Exemple de progiciel à contraintes de confidentialité
Exemple de progiciel à contraintes de preuve / traces

Exemples de « petits » problèmes
Dans la vie personnelle : la sauvegarde de ses données
Dans la vie professionnelle : crash d'un serveur

2.8.2. Les grands enjeux stratégiques :

- catalogue des risques, accepté par l'institution ;
- catalogue des services formalisés de la DSI et de ses fournisseurs internes et externes ;
- Faire rentrer la DSI dans une démarche d'amélioration continue ;
- intégration de la SSI en amont de tous les projets ;
- Culture de l'analyse des risques et de l'acceptation des risques résiduels ;
- Culture de la procédure ;
- faire comprendre à la DG que la DSI n'est que la MOE de la SSI, la MOA étant les services métier

3. Éléments de stratégie

3.1. La montée en charge de la préoccupation SSI

3.2. Paradigme d'approche

3.3. Le RSSI

3.4. Les relations du RSSI

3.5. Les instances SSI

3.6. Les moyens

Les budgets SI
Les budgets SSI

3.7. Découpage des projets

SMSI
PCA-PRA
IAM
Sauvegarde / restauration
Bloc d'Accès
Sécurisation du parc
Traçabilité
HDS

Audit
Archives
Protection AV
Réseau
Chiffrement
Conformité
Cloud

4. Le SMSI

Parler du socle documentaire

5. Les autres projets

5.1. Le PRA/PCA

5.1.1. Définition

Trois définitions de PCA-PRA

5.1.2. Cadrage

Continuité métier :
- procédures dégradées
- plan de repli utilisateur

Continuité technique
- plan de secours IT + TelCo
- gestion de la disponibilité
- plan de sauvetage des locaux
- plan de secours éditions
- plan de repli DSIT

Plan support
- plan juridique
- plan de communication
- cellule de crise

5.1.3. Architecture technique

Impact sur le bâti

5.1.4. Les composants critiques d'un SI

Schéma RTO/RPO

5.1.5. Les procédures dégradées

5.1.6. Plan de tests

5.1.7. Impacts managériaux

5.2. Le projet IAM (décret confidentialité)

5.2.1. Le contexte

Décret confidentialité, qui impose un moyen d'authentification fort validé GIP-CPS pour l'accès à des données médicales nominatives.

5.2.2. Les fondamentaux

Notion de cryptographie
Notion d'authentification forte
Notion de certificat
Notion de PKI

5.2.3. Les processus métiers impactés

Processus RH pour l'identification des personnels
Processus métiers pour les habilitations

5.2.4. Les briques fonctionnelles

Annuaire agent
Meta annuaire
Provisionning amont et aval
Annuaire d'habilitations
CMS
SSO
FUS
Mode kiosque

5.2.5. Les difficultés

Rendre à la MOA RH la maîtrise des annuaires agents
Rendre aux MOA métiers la maîtrise des règles d'habilitation
Concilier les exigences de sécurité avec les usages dans les Unités de Soins.

5.3. Les sauvegardes

5.4. Le bloc d'Accès

5.5. La sécurisation du parc

5.6. Traçabilité

5.7. Le projet HDS

5.8. Les audits

5.9. L'archivage numérique

5.10. La protection antivirale

5.11. La protection du réseau

5.12. Le chiffrement

5.13. La conformité

5.14. La protection du Cloud

6. Aspects financiers de la SSI

7. Domaines connexes

Le risque projet

8. Prospectives 2030

Voir SMSI.FORM.Prospectives2030

9. Exercices et mises en situation

9.1. Exemple d'étude au SAMU du CHU de NANTES

Les outils que l'on pensait critique avant l'étude de risque :

- le dossier patient ;
- le téléphone ;

Les outils que se sont révélés critiques après étude de risque
- CR de résultats de Labo
- VIDAL
- Téléphone
- Système de bip
- TPO (transports de petits objets)

10. Annexe 1 : les principales jurisprudences

Arrêt Nikon (cours de cassation, 2 oct 2001) : vie privée résiduelle sur le lieu de travail
« Attendu que **le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée** ; que celle-ci implique en particulier le **secret des correspondances** ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et **ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur**. »

Arrêt Nortel (cours de cassation, 19 mai 2004) : cas d'atteinte à la réputation
Considère qu'un salarié qui, pendant son temps de travail et à partir de la connexion Internet de l'entreprise :
- visitait des sites échangistes et pornographiques,
- alimentait son propre site échangiste et pornographique,
- utilisait sa messagerie professionnelle pour envoyer et recevoir des messages sur des thèmes sexuels ou des propositions échangistes ;
- détourne son ordinateur et la connexion Internet de l'usage pour lequel ils avaient été mis à sa disposition, se rendant coupable de l'infraction pénale d'abus de confiance ;

Cours d'appel de Limoges, 23 février 2009 : encadrement des usages extra-professionnels
Cas des propos préjudiciables tenus auprès de tierces personnes :
- l'Utilisation de cette messagerie pour *« diffuser ses messages à l'ensemble de ses collègues, pour formuler des critiques à l'encontre de leur employeur et les inciter à intenter des actions en justice et à signer une pétition contre celui-ci »*, est une violation de l'obligation de loyauté justifiant un licenciement pour faute grave ;

Caractère exceptionnel de l'usage dans des buts privés :
- « *Faute d'avoir été autorisée ou à tout le moins tolérée par l'employeur* », l'**utilisation** à des fins personnelles de la messagerie électronique interne de l'entreprise mise à la disposition des salariés par l'employeur « *est en soi **fautive** dès lors qu'elle est **habituelle**, voire **systématique** » ;*

Arrêt Lucent (CA Aix en Provence, 13 mars 2006) : mise en jeu de la responsabilité de l'employeur
Les juges déclarent responsable de contrefaçon l'employeur (Lucent Technologies) du créateur d'un site Internet litigieux en constatant que « ***le site litigieux a été réalisé sur le lieu de travail grâce aux moyens fournis par l'entreprise*** » ; que, dans la mesure où la libre consultation des sites Internet était autorisée et aucune interdiction spécifique n'était formulée quant à l´éventuelle réalisation de sites Internet ou de fourniture d'informations sur des pages personnelles, la faute salarié avait été commise dans le cadre des fonctions auxquelles il était employé.

Dans son examen des conditions de l'exonération de la responsabilité de l'employeur, la Cour d'appel a en effet rejeté le moyen de défense soulevé par l'employeur en considérant que :

- *« le préposé, qui avait pour fonction d'effectuer des tests de qualité de fiabilité du matériel « et dans une entreprise dans laquelle l'usage d'un ordinateur et d'Internet est quotidien, a « agi dans le cadre ses fonctions ;*
- *« il a agi avec l'autorisation de son employeur qui dans une note de service avait autorisé « l'utilisation des équipements informatiques mis à leur disposition pour consulter d'autres « sites que ceux présentant un intérêt en relation directe avec leur activité ;*
- *« il n'a pas agi à des fins étrangères à ses attributions, puisque selon le règlement « précité, il était autorisé à disposer d'un accès à Internet, y compris en dehors de ses « heures de travail ;*

Arrêt Cathnet-Science (cours de cassation, 17 mai 2005)
«L'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus dans le disque dur de l'ordinateur qu'en présence de ce dernier ou celui-ci dûment appelé », à moins que cela ne soit justifié par un « risque ou évènement particulier ».

Arrêt « SANOFI-Chimie » (Cass.soc. 17 juin 2009)
Établissement classé SEVESO
L'employeur ayant reçu des lettres anonymes « *faisant état du contenu de courriels ultraconfidentiels et verrouillés et accompagnées de la copie d'un tel courriel* », *lequel avait un libellé « sécurité-sûreté », il en résultait que le système de cryptage et de protection des données de l'entreprise avait été forcé et ce en méconnaissance de sa charte informatique »*.

Arrêt TECHNI-SOFT (18 octobre 2006) : droit d'accès aux données professionnelles : présomption et entrave
« Attendu que les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence. »
Le comportement du salarié qui procède volontairement au chiffrement de son poste informatique, sans autorisation de la société faisant ainsi obstacle à la consultation, constitue une faute grave qui justifie le licenciement.

Cass.soc., 9 juillet 2008, Franck L. / Entreprise Martin : présomption de caractère professionnel
Attendu de principe : « attendu que les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence ».

Cour d'appel de Paris, 17 décembre 2001 (PMMH/ESPCI)

- Notion d'interception de correspondances : « ne constituent pas une interception la lecture et la retranscription de messages dès lors que celles-ci ne nécessitent ni dérivation ou branchement et sont effectuées sans artifice ni stratagème ».
- Limites des pouvoirs des administrateurs :

« Il est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité ce qui entraîne, entre autre, qu'ils aient accès aux messageries et à leur contenu, ne serait-ce que pour les débloquer ou éviter des démarches hostiles. Ils ont donc un accès courant au réseau sans avoir besoin d'une quelconque manœuvre ».
« La préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de

réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait - de la même façon que la poste doit réagir à un colis ou une lettre suspecte. Par contre, la divulgation du contenu des messages (…) ne relevait pas de ces objectifs. »

CA Paris, 4 février 2005 (WPO / BNP Paribas) : position de FAI d'un hôpital
Qualité de prestataire technique (fourniture d'accès à l'Internet auprès de ses employés)
Obligation de conservation des données d'identification des créateurs de contenu et communication sur réquisitions judiciaires

11. Annexe 2 : FAQ sur des cas pratiques

Concernant les données stockées sur le réseau par un utilisateur dans son dossier personnel (u:) ainsi que sa messagerie, notamment sur l'accès aux données par une autre personne en cas d'absence/départ de la personne :

- Qui a autorité pour donner un accord pour accéder à ces données ?
  - Droit d'accès de l'employeur aux données présumées à caractère professionnelle > accord/gestion du supérieur hiérarchique eu égard à la continuité du service
  - Cas d'accès aux données personnelles (3) :
    - Présence de l'Utilisateur
    - Celui-ci dûment appelé
    - Risque ou évènement particulier
- Lors du départ de la personne, a-t-on obligation de conserver les données de cette personne, combien de temps ?
  - Conservation des données Métier (professionnelles) : durée à définir en fonction de l'utilité de ces données
  - Données privées : pas d'obligation de conservation (vocation professionnelle des outils mis à disposition). Généralement, la procédure de départ prévoit que le collaborateur s'assure de la suppression de ces données. A défaut, il est informé que ces données pourront être détruites après son départ.

Photographie pour les cartes CPE : un agent peut-il refuser de se faire photographier ?

- Fondement juridique : art. 9 C. Civil
- Opposabilité du droit à l'image (oui) ex. motifs religieux

Nécessité d'une autorisation spécifique de l'agent (oui)

Contrôle d'identité : qui a le droit d'en faire, quand, comment, … ?

- Pouvoir réservé aux seuls OPJ (dispositions sur les contrôles et vérification d'identité : articles 78-2 et 78-3 C. proc. pénale)
- Loi n°83-629 du 12 juillet 1983 réglementant les activités privées de sécurité (modifiée par la loi du 18 mars 2003 sur la sécurité intérieure)

Disponible sur le site Legifrance : http://www.legifrance.gouv.fr/./affichTexte.do?cidTexte=JORFTEXT000000320194&fastPos=4&fastReqId=2105831028&categorieLien=cid&oldAction=rechTexte

- Pouvoirs limités des personnels de sécurité :

- sauf autorisation préfectorale, action limitée « à l'intérieur des bâtiments ou dans la limite des lieux dont ils ont la garde »
- sauf accord de l'intéressé, pas de fouille ni de contrôle d'identité (simple vérification visuelle du port du badge si règle interne en ce sens)

Quel est le positionnement juridique de la DSIT pour les accès à Internet : sommes-nous assimilables à un provider ?

- La **loi du 23 janvier 2006** sur la lutte contre le terrorisme précise que sont concernées par l'obligation de conservation des données de connexion à l'Internet, « *les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit* » (CPCE, art. L. 34-1, I, al. 2).

- **CA Paris, 4 février 2005 (WPO / BNP Paribas)** : qualité de prestataire technique (fourniture d'accès à l'Internet auprès de ses employés) (oui) – obligation de conservation des données d'identification des créateurs de contenu et communication sur réquisitions judiciaires (oui)

- **Délibération CNIL n° 2005-208 du 10 octobre 2005** portant avis sur le projet de loi relatif à la lutte contre le terrorisme : considère que les entreprises ou administrations qui offrent un accès au réseau à leurs seuls salariés ou agents ne sont pas concernées par l'obligation de conservation des données.

Le support technique, parce que les disques sont pleins, a-t-il le droit de supprimer des données **manifestement non professionnelles** sur les répertoires utilisateurs professionnels (.mp3, photos de mariages, dvd), etc. Sinon quelle est la marche à suivre ?

- Vocation professionnelle des outils mis à disposition des Utilisateurs
- Respect des règles inscrites dans la Charte
- Bonnes pratiques : sauf urgence, avertissement préalable de l'Utilisateur + délai pour sauvegarder/supprimer les données concernées

Focus sur les délais de conservation : décret du 24 mars 2006

Finalité de la conservation des données	Réquisitions judiciaires (art. 34-1, I)	Facturation / commercialisation des services (art. 34-1, II)	Sécurité des réseaux (art. 34-1, III)
Durée légale de conservation	1 an à compter de la date d'enregistrement	Durée utile au traitement dans la limite de 1 an max.	En fonction des besoins et dans la limite de 3 mois maxi.
Nature des données conservée	- Identification de l'utilisateur - Équipements terminaux utilisés - Caractéristiques techniques de la communication, date, horaire et durée	- Identification de l'utilisateur - Équipements terminaux utilisés - Caractéristiques techniques de la communication, date, horaire et durée - Services complémentaires demandés ou utilisés et leurs fournisseurs - données à caractère technique relatives à la	- Origine de la communication - Caractéristiques techniques de la communication, date, horaire et durée - Identification (données techniques) du ou des destinataires de la communication - Services complémentaires demandés ou utilisés et leurs fournisseurs

	- Services complémentaires demandés ou utilisés et leurs fournisseurs - identification du destinataire de la communication (téléphonie) - Origine et localisation de la communication	localisation de la communication, l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation	

12. Annexe 3 : limite des méthodes formelles d'appréciation des risques

Statistiques nucléaire

Nb total de réacteurs dans le monde : environ 500
Age du plus vieux au 01/01/2011 : 44 ans
Probabilité théorie de sinistre : 1/1 000 000 par réacteur et par an, soit un accident de réacteur tous les 2000 ans
Probabilité empirique : 4 accidents en 44 ans (1 Tchernobyl, 3 Fukushima), soit 1 tous les 11 ans

13. Annexe 4 : extrait DSIH juin 2016

Ô lecteur, si tu as cliqué sur ce lien par curiosité, tu te demandes ce que l'on peut bien encore écrire sur ce sujet battu et rebattu. Il se trouve que nous n'allons pas – ou peu – évoquer des aspects techniques, mais plutôt le niveau de maturité sur cette question. Une échelle GARTNER, assez semblable d'ailleurs à celle de COBIT, découpe la maturité en 5 niveaux.

Au niveau initial, dit « basique », la production d'un service IT est réalisée en mode improvisée ; il n'y a pas de documentation, et peu de prévisions. Ô lecteur, si tu t'es contenté de déployer un antivirus sur tes postes de travail, tu n'en es pas plus loin que çà. Quid en effet de l'analyse des PC en erreur (AV local mal déployé, signature pas mise à jour), des infections sur tel ou tel autre PC, des équipements non protégés comme ceux du biomed ?

Au niveau reproductible, dit « réactif », la production est faite en mode pompier : il y a une gestion des évènements. Ô lecteur, si tu analyses systématiquement les infections à postériori mais que tu ne prends aucune mesure à priori pour limiter ces infections (formation, analyse de la typologie des infections pour en réduite la fréquence), tu en es là.

Au niveau défini, dit « proactif », la production de service IT est réalisée en mode industriel. Il y a une automatisation des taches, une réduction systématique de la complexité, une analyse et une surveillance des tendances. Si, en plus des niveaux précédents, tu as ô lecteur mis en place un mécanisme automatique permettant de comparer la liste des équipements connus de ton antivirus et ceux présents sur le LAN (le delta correspondants aux équipements non protégés), si tu as des

actions systématique d'analyse et de traitement des équipements non protégés avec une réduction du risque et identification des zones résiduelles, tu en es là.

Au niveau mesuré, dit « systématique », tu es capable ô lecteur de sortir des indicateurs en mode presse bouton pour n'importe quel auditeur externe ou pour ta direction générale, concernant le sujet de la protection antivirale, incluant bien évidemment les équipements de la DMZ, les équipements nomades, etc.

Enfin au niveau optimisé, dit « Valeur », la production de service est corrélée aux objectifs de l'entreprise. Si tu en es là ô lecteur, c'est que tu as réussi à expliquer à ta direction générale que la protection antivirale apporte de la valeur car elle consolide la confiance des acteurs dans le SI de l'entreprise.