Côté cours : Le métier de responsable de la sécurité des systèmes d'information

Description du thème

Propriétés	Description
Intitulé long	Le métier de responsable de la sécurité des systèmes d'information : dialogue avec un professionnel
Formation concernée	BTS Services Informatiques aux Organisations
Matière	Analyse économique, juridique et managériale des services informatiques
Présentation	Décrire en quelques phrases les objectifs et la progression
Notions	Thème D5 - La sécurité des systèmes d'information Thème D6 - La responsabilité des prestataires internes et externes du SI Thème EM 4 - Le système d'information (SI) et les processus de l'organisation (décisionnels, opérationnels)
Transversalité	SI5, SI7, SISR3, SISR4
Pré-requis	Différents types de contrats de travail (D2.2) Principes généraux des contrats (D3.1) Les différents types de contrats liés à la production et la fourniture de services (D3.2) Le choix d'externaliser, l'échange et le contrat (EM1.4) Le rôle des normes et standards dans le secteur informatique (EM2.3)
Mots-clés	Système d'information ; sécurité informatique ; charte informatique ; patrimoine informationnel ; protection des données ; responsabilité professionnelle, contractuelle, pénale ; contrat ; externalisation informatique.
Auteur(es)	Sylvie Vonarx. Remerciements à Y. Barrau, A. Guillon-Drouelle, M. L'Helguen et A. Osswald pour leurs lectures, remarques et modifications fructueuses.
Version	v 1.0
Date de publication	Novembre 2015

Un responsable Systèmes et sécurité évoque son métier

I Préambule

1 État des lieux : De nouveaux enjeux pour les responsables informatiques

Cet état des lieux a pour but de cerner les « contours » du ***métier du responsable informatique*** *qui intervient dans un* ***contexte très évolutif*** *qui connaît des avancées technologiques permanentes.*

Face aux **évolutions technologiques, à la virtualisation** (*smartphones* plus performants, connectés et multi usages, tablettes, services *cloud* et réseaux sociaux) ainsi que face à la criminalité informatique dont les risques sont avérés, de nouveaux enjeux apparaissent qui amènent les organisations non seulement à prendre conscience des menaces mais aussi à déployer, par anticipation, **une politique efficiente de gestion des risques et de sécurité**. Les enjeux de **la sécurité informatique** sont au cœur de la stratégie des organisations afin de **protéger le patrimoine informationnel et de respecter les obligations légales** concernant non seulement les données à caractère personnel mais, de manière générale, toute information issue d'un traitement informatique. **La croissance exponentielle** des attaques, le vol et la perte de données, les intrusions dans les systèmes d'information, une panne d'électricité dans un *datacenter*[1] ou un incendie, une inondation, tous ces dangers sont de plus en plus prégnants et ne peuvent plus être ignorés.

Aussi, en raison de **l'évolution des usages et pratiques**, la **barrière périmétrique des infrastructures** disparaît-elle avec la multiplication des plateformes mobiles et le développement de l'informatique en nuage (*cloud*). Pour y répondre **les organisations se dotent d'outils pour sécuriser** les terminaux mobiles multi-OS : effacement des données à distance, verrouillage à distance, activation d'un accès par mot de passe, cryptage, authentification, mise en place d'un pare-feu, antivirus et VPN[2] (*Virtual Private Network*) mobile. Pour le *cloud*, **les clauses spécifiques des contrats d'hébergements et le cahier des charges associé** permettent **au prestataire et au client** de déterminer non seulement le **niveau de sécurité** mais aussi **les responsabilités respectives**.

Ensuite, afin de faire face aux conséquences pour l'activité des entreprises, celles-ci s'organisent pour assurer un **plan de continuité d'activité (PCA)** et **préserver ainsi leur capacité à poursuivre leurs activités** malgré la survenance d'un sinistre majeur. La **restauration** rapide des services ou **du réseau informatique** permet d'éviter de graves conséquences économiques, juridiques mais aussi en termes d'image (gestion efficace de crise, persistance de la confiance et fidélisation des clients…). Enfin, les entreprises peuvent obtenir la certification de leur **PCA** sur le fondement de **la norme internationale ISO 22301**. Dans le cadre de la procédure de certification du PCA seront pris en considération : l'évolution des *datacenters* et la mise en place **d'un site de secours ou de repli** permettant la bascule complète d'un *datacenter*.

Ainsi pour assurer la continuité de leurs activités, pour protéger leur patrimoine informationnel (données financières, stratégiques, à forte valeur ajoutée) et les données à

[1] Datacenter : centre de données est un endroit physique où sont rassemblées de nombreuses machines (serveurs) contenant des données informatiques.

[2] VPN : Interconnexion de réseaux locaux via une technique de tunnel sécurisé, généralement via internet.

caractère personnel, les organisations déterminent, dans le cadre de leur politique de sécurité numérique, **leurs objectifs** en matière de **gestion des risques**, les **normes applicables** et mettent en place des **procédures en respect des règlementations**.

C'est dans ce contexte qu'intervient en classe un professionnel de la sécurité et des systèmes d'information.

J'ai tout d'abord rencontré M. Osswald en 2014, lors du jury BTS SIO puis lors des évaluations concernant la validation des acquis de l'expérience (VAE). Nous avions déjà réalisé une telle expérience en invitant le responsable informatique de la Direction Départementale du Territoire (DDT, organisation publique) pour une présentation des activités menées au sein de cette organisation.

M. Oswald est titulaire d'un BTS en informatique. Il totalise 23 années d'expérience en sociétés de services. Il est, depuis 2007, responsable Systèmes et sécurité d'un organisme financier. Dans le cadre des activités de formation, M. Osswald intervient pour la validation des acquis de l'expérience (VAE, reconnue par le Code du travail) et pour l'évaluation de l'épreuve E4 (parcours de professionnalisation). Il participe de même au jury BTS SIO.

Vous pourrez prendre connaissance du profil de M. Osswald responsable sécurité et systèmes (page 4) puis l'essentiel des propos qu'il a tenus lors de sa conférence du 10 février 2015 (page 5) Enfin, vous pourrez lire les échanges nés de l'entretien auquel il a participé (page 13).

2 Adéquation avec le programme SIO et complément pédagogique

La conférence de M. Osswald (le compte-rendu se trouve dès la page 5) s'inscrit dans les thèmes suivants du programme de l'enseignement EDM :

- ✓ Thème D5 - La sécurité des systèmes d'information
- ✓ Thème D6 - La responsabilité des prestataires internes et externes du SI
- ✓ Thème EM 4 - Le système d'information (SI) et les processus de l'organisation (décisionnels, opérationnels)

Ces thèmes sont ceux des spécialités SISR et SLAM du BTS SIO.

Le fait d'associer des professionnels comme M. Oswald dans le cadre de l'analyse économique, managériale et juridique des services informatiques aux organisations[3] en BTS SIO correspond tout à fait aux spécificités de cet enseignement (approche par les cas, contextes professionnels…).

Par ailleurs, les problématiques actuelles liées au *Big Data*[4], à l'internet des objets, au développement du *cloud*, etc. ont un impact de plus en plus important sur la sécurité des systèmes d'information. Ce qu'il est nécessaire de prendre en compte dans nos enseignements.

[3] Analyse économique, managériale et juridique des services informatiques aux organisations ou EDM = économie, droit, management.

[4] Big Data : désigne des ensembles de données qui deviennent tellement volumineux qu'ils en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information.

Enfin la compréhension d'un véritable contexte professionnel, qui induit de réelles problématiques, s'avère déterminante pour conduire nos activités en classe.

Fort de ce constat et en s'appuyant sur cet entretien avec M. Osswald, nous pouvons dégager plusieurs thématiques :

- L'impact des contraintes légales dans les organisations,
- L'utilité de la veille juridique,
- Le responsable Sécurité du système d'information et les missions fixées par la DG (aspects juridiques),
- Le *cloud* : définition du niveau de sécurité et responsabilité dans les contrats,
- La gestion de la confidentialité : comment ? quels outils ? En réponse à quelle contrainte ?
- Externalisation : pourquoi et comment ?
- L'acquisition d'outils (protection des réseaux),
- L'importance des normes,
- Les règles organisationnelles et techniques,
- L'appartenance des matériels exploités (BYOD → *Bring your own device*, CYOD → *Choose your own device*, COPE → *Company-issued, personnaly-enabled*) : mise en place et protection des données à caractère personnel par exemple.

II Le profil du professionnel rencontré

Trente années d'expérience dans l'élaboration de SI[5], la gestion des systèmes et des réseaux ainsi que dans la conception et le développement d'applications**.**

Voici un résumé de son *curriculum vitae* :

Depuis 2007 – SADE filiale de BGL BNP Paribas
Responsable systèmes et sécurité

- En charge de l'infrastructure réseau, matérielle et de la sécurité des systèmes
- Définition et conception du PRI[6] (site de production – site de secours – bascule et retour arrière)
- Spécification et conception (logiciel métier)
- Migration BI (BO vers MyReport)
- Prise en compte des règlementations bancaires
- Backup du DSI (contrats, budgets, comités)
- Communication en anglais avec le groupe

De 1991 à 2007 – ARES-Est
Responsable technique

- Encadrement de l'équipe technique (15 personnes)
- Mise en place des progiciels de la gamme Arcole
- DBA Oracle

[5] SI : système d'information
[6] Plan de reprise informatique (PRI)

- Gestion de projets techniques et fonctionnels
- Animation de séminaires et support commercial
- Réalisation de développements spécifiques
- Audits d'exploitation et de sécurité

De 1989 à 1991 – InfoTeam
Chef de projet

- Vente et réalisation de spécifiques
- Suivi et démarrage de plates-formes matérielles
- Formations

De 1987 à 1989 – Promo-Informatique (groupe BECM)
Chef de projet

- Projets de développement
- Installation et migration de systèmes

De 1984 à 1987 – SemaGroup (groupe BNP Paribas)
Analyste-programmeur

Les compétences spécifiques :

Forte technicité

- Réseau et sécurité
- Applications publiées Citrix XenApp
- Virtualisation (VMWare – HyperV)
- Sauvegarde VEEAM
- SGBDR Oracle
- Outils de développement
- Décisionnel (MyReport – BO)

Adaptabilité

- Prise en compte globale des projets
- Gestion des ressources
- Relationnel utilisateurs

III Conférence de M. André Osswald, Responsable Systèmes et sécurité, Groupe SADE (organisme financier qui appartient à la BNP)

Les pages suivantes permettent de découvrir la synthèse de la conférence.

La protection des systèmes d'information est un thème majeur de nos jours. Trois pôles essentiels ont été traités et sont illustrés par des exemples :

1er pôle : **les contraintes** (environnementales, matérielles, légales, liées à l'entreprise, liées aux utilisateurs).

2ème pôle : **les parties prenantes et les normes** (direction générale, ISO 27002, RSSI – responsable homme clé).

3ème pôle : **les niveaux et méthodologie de sécurisation du SI** (physique des matériels, de l'environnement, logique, des applications, des réseaux).

Chaque pôle est composé de plusieurs sous-parties. Un résumé figure à la fin de chaque sous-partie afin de favoriser une vision synthétique des notions abordées.

1 1er pôle : les contraintes liées à la protection des systèmes d'information

Le **site informatique (**que ce soit de gestion ou de production) **interne à l'organisation** peut être exposé à des **risques géographiques et/ou environnementaux**. L'implantation d'un site de repli ou de secours est obligatoire et cette règle doit être respectée. Le site de repli doit être à distance du site à protéger. Par exemple, le site de repli de certaines sociétés situées dans l'une des *Twin Towers* (de l'ex *World Trade Center*) était localisé dans la seconde tour. Pour le groupe Sade (situé à Strasbourg), le site de secours a été, dans un premier temps implanté à Mulhouse, pour l'être ensuite à Paris (distance exigée dans le monde bancaire : minimum 400 km).

Lorsque **la décision d'externaliser est prise**, il convient d'être très vigilant quant aux termes du contrat en ce qui concerne les droits d'accès aux locaux, les certifications ou encore le lieu du stockage effectif des données (choix de l'hébergeur et connaissance de la destination finale des données en cas d'externalisation en cascade).

Pour les **salles « vertes » (l'informatique verte ou durable** vise à réduire l'empreinte économique, écologique et sociale des TIC**),** le recours à la **virtualisation** permet des gains de place et des économies d'énergie. L'arrêt des machines utilisateurs constitue un premier niveau de sécurité lors de la survenance d'un risque. Pour le développement (SOA[7] vs monolithe[8]) et afin de répondre aux besoins de conception, des solutions existent telles que le partage et petits modules accessibles à la demande. S'agissant des droits d'accès, ceux-ci doivent être considérés tant au plan physique que logique et toute action doit être tracée.

Résumé : les différentes contraintes de site :

- *Contraintes internes (localisation dans l'entreprise, risques environnementaux, risques géographiques)*
- *Contraintes externes (choix de l'hébergeur, mise en place d'un contrat)*
- *Droits d'accès*
- *Site de secours (respect d'une distance géographique)*
- *Salle verte (réduire la consommation d'énergie, virtualisation des infrastructures, améliorer la sécurité, optimiser la place, améliorer le confort, simplifier la conception, accès et sauvegarde distants)*

La **gestion du portefeuille des équipements** (cartographie) permet en outre de prévoir le renouvellement (à budgéter) et permet de garantir la compatibilité des systèmes et leur support. Dans le cas d'un **système embarqué** (exemple : le téléphone portable qui contient un

[7] SOA : en génie logiciel, une application SOA (Architecture orientée services) est une application constituée de divers services distants. Un service est une application distante offerte par un fournisseur à un client basée sur une relation de confiance.

[8] Monolithe : En génie logiciel, une application monolithique décrit une architecture logicielle dans laquelle l'interface utilisateur et le code d'accès aux données sont combinés en un seul programme sans modularité.

champ personnel et un champ professionnel), il s'agit de sécuriser : en cas de perte ou de vol, les données professionnelles devront pouvoir être effacées à distance.

Résumé : Les contraintes matérielles :

- *Gestion du portefeuille des équipements*
- *Renouvellement*
- *Interopérabilité*
- *Maintenance*
- *Fragilité*

L'archivage et la conservation des données sont règlementés (exemples des données salariales ou des enregistrements vidéo). Les données financières à déclarer, par exemple, les services fiscaux requièrent trois années réglementaires plus l'année en cours pour le fichier des écritures comptables (FEC, à présenter aux contrôleurs de l'administration fiscale). Les contraintes légales sont liées au domaine d'activité (contraintes pour la finance ou pour la défense). Enfin des normes sont imposées comme, par exemple, pour les activités de santé.

***Résumé : Les contraintes légales** :*

- *Archivage et conservation de certaines données (données salariales, vidéo-enregistrements)*
- *Déclaratifs (organismes de régulation, réglementaires)*
- *Domaine d'activité*
- *Normes imposées*

En matière de disponibilité, la direction détermine le **délai d'interruption et le niveau de perte de données acceptables** ; ces indicateurs sont fonction de l'activité de l'entreprise (site marchand, *datacenter*, …). Le travail du responsable consiste à définir (sous contrainte de budget) les performances attendues (temps de réponse et pics de connexion), à vérifier l'intégrité des données, leur protection et les traces d'altération[9]. En ce qui concerne la confidentialité, il s'agit d'organiser la **gestion des accès** : le responsable gère les moyens mais pas les contenus qui sont gérés par les administrateurs des applications (l'administrateur système n'est pas l'administrateur des données). La confidentialité peut être renforcée par le recours au cryptage.

Résumé** : **les contraintes liées à l'entreprise :

- *Disponibilité (délai d'interruption toléré, perte de données tolérée)*
- *Budget (analyse des données sensibles, performances attendues, étude des outils)*
- *Intégrité (protection des données, traces d'altération → pas de trace / valeur avant-après / retour à la valeur précédente automatique)*
- *Confidentialité (gestion des accès, cryptage)*

La propriété des matériels utilisés (**BYOD** → *Bring your own device*, **CYOD** → *Choose your own device*, **COPE** → *Company-issued, personnaly-enabled*) est à considérer en termes de sécurité (exemple authentification à un domaine d'accès au WiFi ou sur un réseau d'invité, durée de conservation des accès sur un an). La **variété des postes (**PC classique, portable, client léger, mobile) nécessite des modules de protection variables selon le matériel et le **profil de travail (partages des postes ou encore télétravail).**

[9] On distingue 3 niveaux : pas de trace, ou valeur avant-après, retour à la valeur précédente.

Résumé : les contraintes liées aux utilisateurs :

- *Appartenance des matériels utilisés (BYOD → Bring your own device, CYOD → Choose your own device, COPE → Company-issued, personally-enabled)*
- *Variété des postes de travail*
- *Profils de travail (partage des postes, télétravail)*

Dans ce premier pôle, les étudiants ont pu découvrir une vision synoptique des contraintes dans une organisation.

2 2ème pôle : les parties prenantes et le rôle des normes

C'est la **Direction Générale** (DG) qui élabore la **démarche globale** (performances et budgets en adéquation) et la **vision stratégique** en termes de disponibilité et vis-à-vis des clients (rassurer les clients sur la sécurité de l'entreprise). Elle détermine **la politique SSI (Sécurité du système d'information)**, les éléments stratégiques (domaines vitaux), les directives, les procédures et codes de conduite (chartes) ainsi que les règles organisationnelles et techniques. En continuité, la DG gère **l'évolution** de la **politique du SSI** pour les **changements du contexte** (organisation de l'entreprise, missions et audits) et **l'analyse des risques** (réévaluations des menaces).

Enfin, la DG assume **le leadership de la sécurité** (sensibilisation, communication interne et externe, formations aux utilisateurs) et prouve par ses actions, l'importance qu'elle accorde à la SSI.

Résumé :* la *Direction générale :

- *élabore la démarche globale (performances et budgets adéquats, vision stratégique)*
- *détermine la politique SSI (sécurité du système d'information)*
- *gère l'évolution de la politique du SSI (changements de contexte, analyse des risques)*
- *assume le leadership de la sécurité (sensibilisation, communication, formation)*
- *prouve par ses actions l'importance qu'elle accorde à la SSI*

L'homme clé est le responsable SSI (RSSI) rattaché initialement à la DSI, il est, de nos jours, rattaché de plus en plus à la DG. Le RSSI traite des systèmes d'informations complexes et gère le réseau dans sa globalité (LAN, WAN, mobile). Il assume aussi le rôle de conseil dans la définition des procédures et il se charge des missions fixées par la DG (notamment dans les aspects juridiques). **Il est le garant de l'application de la politique de SSI** : sécurité des réseaux et télécommunications, des systèmes des applications, sécurité physique, sécurité des données (sauvegardes), PSI (plan de sécurité informatique) et assume des missions de veille technologique.

Résumé : le RSS, un personnage clé dans l'organisation

- *rattaché au départ à la DSI et de nos jours il est rattaché à la Direction Générale*
- *traite des systèmes d'informations complexes*
- *gestion du réseau dans sa globalité (LAN – WAN – mobile)*
- *rôle de conseil dans la définition de la politique de sécurité*
- *en charge des missions fixées par la Direction Générale*
- *garant de l'application de la politique de SSI*
- *assure les veilles technologique et réglementaire*

Le rôle des normes est déterminant pour ces questions de sécurité du SI. Il faut cependant noter qu'elles évoluent en permanence (par exemple, **la norme ISO 22301** est le nouveau standard international de management de la continuité de l'activité) et qu'il faut donc rester vigilant. Par ailleurs, il existe des normes qui vont permettre de structurer les règles de sécurité. Un exemple de **structuration des règles de sécurité** consiste dans la **norme 27002** (concernant la sécurité de l'information) publiée en 2005 par l'ISO (l'ISO/CEI 27002 est un ensemble de 133 mesures dites *best practices* -bonnes pratiques-) qui s'avère essentielle pour la gestion de la continuité des activités.

Résumé : un exemple, la norme ISO 27002

- *Politique de sécurité*
- *Organisation de la sécurité de l'information*
- *Gestion des biens*
- *Sécurité des ressources humaines*
- *Contrôle d'accès*
- *Acquisition, développement et maintenance des SI*
- *Gestion des services et incidents*
- *Conformité*

Les étudiants ont pu appréhender la place du responsable sécurité et systèmes dans l'organisation, le rôle stratégique qui lui incombe ainsi que son rattachement à la Direction Générale dont les missions sont indiquées.

3 3ème pôle : les niveaux et méthodologie de sécurisation du SI

On distingue plusieurs niveaux de sécurisation :

La **sécurisation physique des matériels** : pour tout le câblage (électrique et informatique), il s'agit de respecter des normes de sécurité. Pour la protection des systèmes, prévoir, en cas d'incendie, une extinction automatique. Pour la température, installer une climatisation si nécessaire. Pour les fluides, un plancher surélevé est plus indiqué en cas d'inondation et éviter tout passage aérien au-dessus du matériel (par exemple s'abstenir de placer des serveurs sous ou à proximité d'une conduite d'eau).

L'importance de la **redondance physique** pour les arrivées électriques, les onduleurs et les composants (alimentation, ventilateurs, disque, cartes réseau) des serveurs, les baies de disques, les accès internet (de préférence avec des FAI[10] différents) est à mentionner. Un exemple à la MGEN de Nancy : le site de secours se trouve dans un local attenant au site principal et ce centre avait demandé à EDF une seconde arrivée électrique (chemin physique différent, en cas de coupure sur la première ligne électrique).

La **protection des accès** (identification et sécurisation) : intégrer qu'il faut être en mesure d'identifier la personne qui est à l'origine d'une action. La salle machine ne doit pas être ouverte en permanence et il faut pouvoir en tracer les accès (voir mettre en place un système de contrôle, d'accès par badge, par exemple).

Le **plan de maintenance préventif** : le site de repli ou de secours doit être testé régulièrement, ainsi que les onduleurs et les procédures à mener. En réseau et système, un

[10] FAI : fournisseurs d'accès à internet

cluster est une grappe de serveurs ou « ferme de calcul » constituée de deux serveurs au minimum (appelés aussi nœuds) et pouvant partager une ou plusieurs baies de disques[11]. Le cluster actif-passif (l'actif est en activité et s'il tombe en panne, le passif prend le relais) ; on peut opter pour un système actif-actif mais il s'agit d'acquérir une seconde licence car les éditeurs imposent souvent l'achat de licence sur tous les nœuds actifs d'un cluster.

Le **plan de maintenance correctif :** mise en place de contrats de maintenance avec délais d'interruption acceptés (choix 24h/24 ou jours de la semaine → choix RTO et RPO (en complément voir RTO/RPO : les indicateurs de sécurité en cas de sinistre).

Résumé : Sécurisation physique des matériels:

- *Respect des normes de sécurité*
- *Protection des systèmes (incendies, température, fluides)*
- *Redondance physique (arrivées électriques, onduleurs, cluster)*
- *Protection des accès (identification et sécurisation)*
- *Plan de maintenance préventif et correctif*

Pour la sécurisation de l'environnement : suivi des mises à jour des systèmes et applications (la mise à jour des systèmes est à planifier, mise à jour des applications pour des raisons légales et/ou règlementaires), gestion du parc (obsolescence) prévoir le coût (contrat de maintenance sur 3 ans voire 5 ans). La DG va intégrer un budget en vue du renouvellement du matériel. Le plan de sauvegarde est à gérer en local et sur le site de secours. Des tests doivent être réalisés en amont afin d'être en mesure d'activer le PSI à distance en cas de besoin. Le PCA (plan de continuité d'activité) et le PRI (plan de reprise informatique) : il est essentiel de prévoir la **réversibilité**, chez l'hébergeur, dans le contrat (clause de réversibilité) afin de déterminer les conditions du rapatriement des données et/ou les matériels. Il est un exemple au Royaume-Uni où l'hébergeur était en faillite et les entreprises n'avaient plus accès à leurs données !

L'exemple de Dropbox où les données des utilisateurs du *cloud* sont consultables par des tiers agréés car cette société est soumise au *Patriot Act*[12] (stockage des données aux USA).

Le *cloud* souverain (exemple des données hébergées) : le *cloud* dit souverain garantit le lieu de stockage. Votre prestataire est dans l'obligation de vous indiquer le lieu d'hébergement de vos données afin que vous puissiez déterminer les législations en vigueur.

Résumé : Sécurisation de l'environnement :

- *Suivi des mises à jour des systèmes et applications*
- *Gestion du parc (obsolescence)*
- *Plan de sauvegarde*
- *Plan de secours*
- *Plan de continuation de l'activité*
- *Plan de reprise*

[11] Source Wikipedia

[12] USA Patriot Act : loi votée par le Congrès des États-Unis et signée par George W. Bush le 26 octobre 2001. Cette loi est destinée à renforcer la sécurité aux USA en fournissant les outils appropriés pour déceler et contrer le terrorisme.

La sécurisation logique (par procédures d'identification notamment) : suivi des comptes d'accès (inventaire – désactivation/suppression) ; prise en compte les droits des personnes (d'accès, de rectification …). La stratégie du mot de passe : (complexité et renouvellement) pensez à 8 caractères au minimum (majuscules, minuscules, chiffres, caractères spéciaux) ! *Single Sign On* (SSO) authentification unique (identification maître, à l'ouverture de la session, tous les autres modules nécessitant une authentification sont en mesure de reconnaître et valider l'accès).

Application de l'**authentification forte pour les accès sensibles/distants** : 3 niveaux de sécurité et certificats. Carte et code pin : deux niveaux de sécurité. Clé USB avec code qui peut être désactivée à distance en cas de perte (utilisation d'un logiciel pour définir une clé et crypter les données). L'identification digitale n'est pas suffisamment fiable car une photo peut reproduire l'empreinte digitale. Carte + nom d'utilisateur + code Pin permet les trois niveaux.

L'organisation des **droits d'accès** : annuaire (groupe *Active Directory* par exemple) et autorité d'assignation des droits.

La **gestion de la confidentialité**, c'est essentiel et l'exemple de **l'affaire Target** dans laquelle les données bancaires des clients étaient… non cryptées est révélateur. Target a subi en 2014 un vol de données, touchant environ 100 millions de clients via son fournisseur de climatisation[13].

Pour information, le type de carte de paiement et de crédit le plus répandu aux États-Unis n'est pourvu que d'une simple bande magnétique comparable à la bande d'une cassette audio (comme l'American Express), ce qui facilite les attaques par la technique du *skimming* (captation des données sur la piste). Les cartes à puces utilisées majoritairement en France – et en Europe –, stockent les informations de façon beaucoup plus sécurisée. Voir en complément : « **USA : la chaîne de magasins Target victime d'un énorme vol de données utilisateurs »** [14]

Pour le **contrôle des échanges de données**, si cela passe par des **périphériques USB**, il est conseillé de mettre en œuvre des mécanismes de cryptage et/ou de protection des données exportées. L'accès à ces supports peut également être désactivé. Il convient de tracer les transferts et de contrôler l'**accès via internet** (limitation des volumes et blocage FTP en sortie - attention à HTTPS → comment contrôler un flux sécurisé ? Si on peut en analyser le contenu, il n'est plus sécurisé !).

Pour la **protection antivirale des données** → par serveur et par OS et en fonction du rôle. Il s'agit de mettre en place une protection adaptée au poste.

Résumé : Sécurisation logique:

- *Procédures d'identification (suivi des comptes d'accès, stratégie de mot de passe, authentification forte pour les accès sensibles ou distants)*
- *Organisation des droits d'accès (annuaire, autorité d'assignation des droits)*
- *Gestion de la confidentialité (cryptage des données des cartes bancaires et personnelles, contrôle des échanges des données, accès Internet)*
- *Protection antivirale des données*

[13] http://business.lesechos.fr/directions-numeriques/0203336807596-apres-le-vol-le-temps-des-explications-61311.php

[14] http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-612150-usa-chaine-magasins-target-victime-enorme-vol-donnees-utilisateurs.html

Pour les **méthodologies de développement**, plusieurs **normes** (règle de nommage, ossature des programmes, gestion des versions) sont à mettre en œuvre. Il s'agit, de même, de mener des contrôles permanents des données (facturation *vs* comptabilité, virements *vs* relevés de compte…). Par exemple lorsque la banque fait une enquête sur l'origine des fonds, dans le cas d'un dépôt, d'un virement ou de l'intervention d'un notaire, il n'y a pas de risque car cela passe par la CDC (la Caisse des Dépôts et Consignations).

Les outils sont présents dans les domaines financiers pour la validité des fonds. Des jeux de tests seront conçus par les partenaires, soumis à des panels de testeurs. Ils permettront de valider les meilleures solutions. Souvent les jeux d'essai ou tests sont faits avant le développement. **L'analyse d'un besoin** peut également être fait **à partir du résultat pour remonter à la source** (départ = facture de 1000,00 euros TTC, composée d'une TVA et d'un montant HT ; montant HT composé de …).

Pour les **environnements adéquats**, les **algorithmes asymétriques** assurent la **non-répudiation** (une action donne lieu à un enregistrement/preuve ; impossibilité pour une personne ou une entité engagée par voie informatique de nier, par exemple, d'avoir reçu ou émis un message signé (système utilisant les clés privées et publiques). Le **cryptage** repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder.

Résumé : Sécurisation des applications:

- *Méthodologie de développement (règle de nommage, ossature des programmes, gestion des versions)*
- *Contrôles permanents (contrôle des données)*
- *Jeux de tests (panel de testeurs, évaluer tous les cas, résultats validés par les utilisateurs)*
- *Environnements adéquats (développement, qualification, production)*
- *Non-répudiation (action donne lieu à un enregistrement, traces, audit des traces)*

La **protection des réseaux** (équipements administrables, accès nominatifs, traces de modification et diversification des niveaux de contrôle) **par des outils et méthodes** (firewall, filtrage de la navigation, analyse des flux SMTP, antivirus pour scanner les messages et fichiers téléchargés, accès VPN → tunnel sécurisé permettant à l'utilisateur d'accéder au réseau local depuis l'extérieur ou de relier deux sites distants).

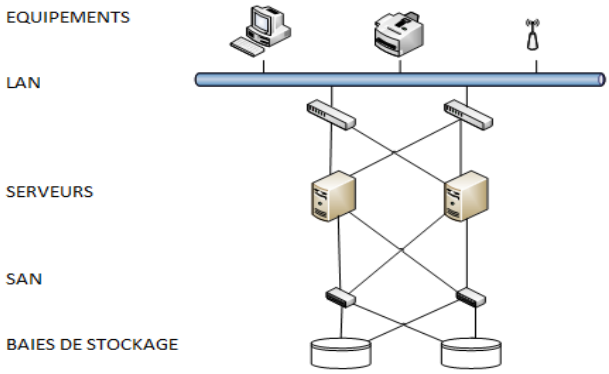
Journalisation du trafic : remontée d'alertes en temps réel, analyse des journaux – contrôle des sites accédés, volume des messages, volume par utilisateur et/ou poste. Par exemple, la haute fréquence d'envoi de courriels peut déclencher une alerte.

Baie de disque : stockage de données connecté à un SAN (un **réseau de stockage**, ou **SAN** de l'anglais - *Storage Area Network*-, est un réseau spécialisé permettant de mutualiser des ressources de stockage), lui-même connecté à un ou plusieurs serveurs (basculement possible entre les serveurs) en s'appuyant sur des **connexions croisées** (voir **image 1 page 13**).

Résumé : Sécurisation des réseaux :

- *Protection des réseaux (équipements administrables, accès nominatifs, traces des modifications de configuration)*
- *Protection des accès (DMZ, multiplication et diversification des niveaux de contrôle, accès VPN)*
- *Journalisation du trafic (remontée d'alertes en temps réel, analyse des journaux)*
- *Basculement possible entre les serveurs en s'appuyant sur des connexions croisées*

Image 1 : Exemple de configuration locale



Pour conclure : les étudiants ont pu partager l'expérience professionnelle du métier dans sa complexité et dans sa mise en œuvre. La présentation s'est terminée à l'issue des questions posées par les étudiants.
Voici une remarque formulée par les étudiants SIO 2ème année : « intéressant, très complet et dense, dynamique, d'une grande limpidité, fluide, pertinent, très détaillé, concis, compréhensible, les exemples apportent l'aspect concret ».

L'ensemble des propos tenus lors de la conférence du 10 février 2015 au lycée Camille Sée à Colmar (68000) ainsi que les exemples et situations décrites sont publiés sur le site web du réseau Certa avec l'accord explicite de M. Osswald.

IV L'entretien avec M. André Osswald, Responsable Systèmes et sécurité, Groupe SADE (organisme financier qui appartient à la BNP)

Sylvie Vonarx (SV) : Bonjour M. Osswald et merci pour le temps consacré à présenter votre métier aux étudiants du BTS SIO de Colmar. Lors de votre présentation, vous avez privilégié une approche en termes de contraintes, puis de ressources et enfin de moyens. Pourquoi avez-vous adopté cette démarche ?

André Osswald (AO) : La formation dispensée dans le cadre du BTS SIO a pour objectif **la présentation des technologies actuellement exploitées**, l'enseignement des méthodes permettant l'utilisation de certaines de ces technologies ainsi qu'une **formation généraliste à l'environnement du monde des entreprises**. La présentation réalisée a permis aux étudiants de découvrir **le spectre complet** couvert par les points à prendre en compte dans la gestion du

le système d'information (SI) d'une entreprise en abordant **les contraintes, les ressources** et **les moyens de sécurisation** (sans entrer dans les détails techniques).

***SV* : Quelle est l'importance des contraintes** ?

OA : Ce sont les contraintes qui définissent le système d'information de l'entreprise : en effet, on ne fait pas de l'informatique pour le plaisir de faire de l'informatique ! À la base, il y **a les besoins** :

- exprimés par **les utilisateurs** ➔ comptabilité, gestion des commandes, gestion du stock, la facturation, …

- exprimés par **la direction** ➔ suivi et pilotage de l'activité, budget alloué, visibilité de l'entreprise, sites internet, intranet ou extranet,…

- liés à la **législation** et/ou à la règlementation ➔ fiscalité, déclaratifs, archivages obligatoires,…

Mis bout à bout**, ces besoins** définissent **les contraintes du SI** en termes de **domaines à traiter, de performance et de disponibilité.**

SV : Oui et la législation est omniprésente. Les établissements financiers ont, par exemple, l'obligation réglementaire de disposer d'un **Plan de continuité d'activité**. Dans ce cadre comment définissez-vous **la mise en place d'un site de repli/secours** ?

AO : Face à un sinistre, notre organisation doit être **apte à assurer la continuité de ses activités**. Ce site de repli/secours doit pouvoir **prendre le relais** en cas d'arrêt du site de production. Aujourd'hui la distance imposée entre deux sites est un minimum de 400 km dans le monde bancaire (pour assurer le relais en cas de risques environnementaux ou autre). Le **RTO (***Recovery Time Objective***)**, à savoir le **délai d'interruption admissible** ainsi que le **RPO (***Recovery Point Objective),* à savoir **la perte de données tolérée**, sont fixés par l'entreprise. Ces deux **indicateurs** permettent de cibler **la solution technique** et de quantifier **la charge financière** à allouer au projet.

Si **l'entreprise s'interdit l'externalisation** d'informations (qu'il s'agisse du site de production ou du site de repli/secours), **l'architecture physique du SI** sera implantée dans des locaux qui lui appartiennent et c'est à elle d'en **assurer/assumer la sécurité**.

Dans le cas contraire**, l'hébergement de l'architecture physique du SI** (appartenant ou non à l'entreprise) doit faire l'objet d'une étude complète permettant d'assurer un niveau **de sécurité correspondant à la politique de sécurité de l'entreprise.**

SV : Vous précisez **les moyens** dans la dernière partie de votre conférence. Pour quelle raison ?

AO : Les moyens sont un aperçu **des solutions que l'on peut mettre en place pour répondre aux contraintes** de l'entreprise. Il s'agit en fait d'outils auxquels les étudiants seront confrontés quotidiennement lorsqu'ils seront en poste.

SV : Votre intervention auprès des étudiants permet à juste titre de **cerner l'activité métier** par votre regard et votre expérience. C'est une « plus-value », si je puis m'exprimer ainsi, et nous en sommes très reconnaissants.

AO : Oui en effet ma présentation permet de faire **le lien entre l'enseignement prodigué aux étudiants et l'activité réelle de l'informaticien au sein d'une entreprise**. Je suis passé par le même cursus (il y a plus de 30 ans, c'est vrai), mais il y avait à l'époque un gouffre entre l'enseignement que j'avais eu et **les tâches qui m'avaient été confiées** dans les entreprises dans lesquelles j'ai travaillé. De plus, durant mon intervention, j'ai pu mettre l'accent sur des points que les étudiants ne jugeaient pas nécessairement importants et **évoquer des tâches de leur futur travail** dont ils ignoraient l'existence. À cette phase de leur formation, les étudiants ne voient que les aspects « bassement » techniques (ils en sont au stade où ils font de la technique pour la technique) et ne sont pas capables de prendre de la hauteur pour appréhender **l'entreprise dans sa globalité**.

SITOGRAPHIE:

http://www.equinox-cognizant.com/wp-content/uploads/2012/12/brochure_pca.pdf
http://www.journaldunet.com/solutions/expert/54193/un-plan-de-continuite-d-activite-operationnel-ne-s-improvise-pas.shtml
http://www.journaldunet.com/solutions/systemes-reseaux/analyse/rto-rpo-les-indicateurs-de-securite-en-cas-de-sinistre.shtml http://www.aps-voxy.fr/rto-rpo-quels-moyens-faut-il-pour-tenir-ces-objectifs/
Target a subi en 2014 un vol de données, touchant environ 100 millions de clients via son fournisseur de climatisation.
http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-612150-usa-chaine-magasins-target-victime-enorme-vol-donnees-utilisateurs.html
http://pecb.org/iso22301fr/
http://www.solucominsight.fr/2011/09/iso-22301-un-nouvel-elan-pour-la-continuite-d%E2%80%99activite/
http://www.llisnetwork.fr/Files/29_llis_network_cablage_informatique.pdf