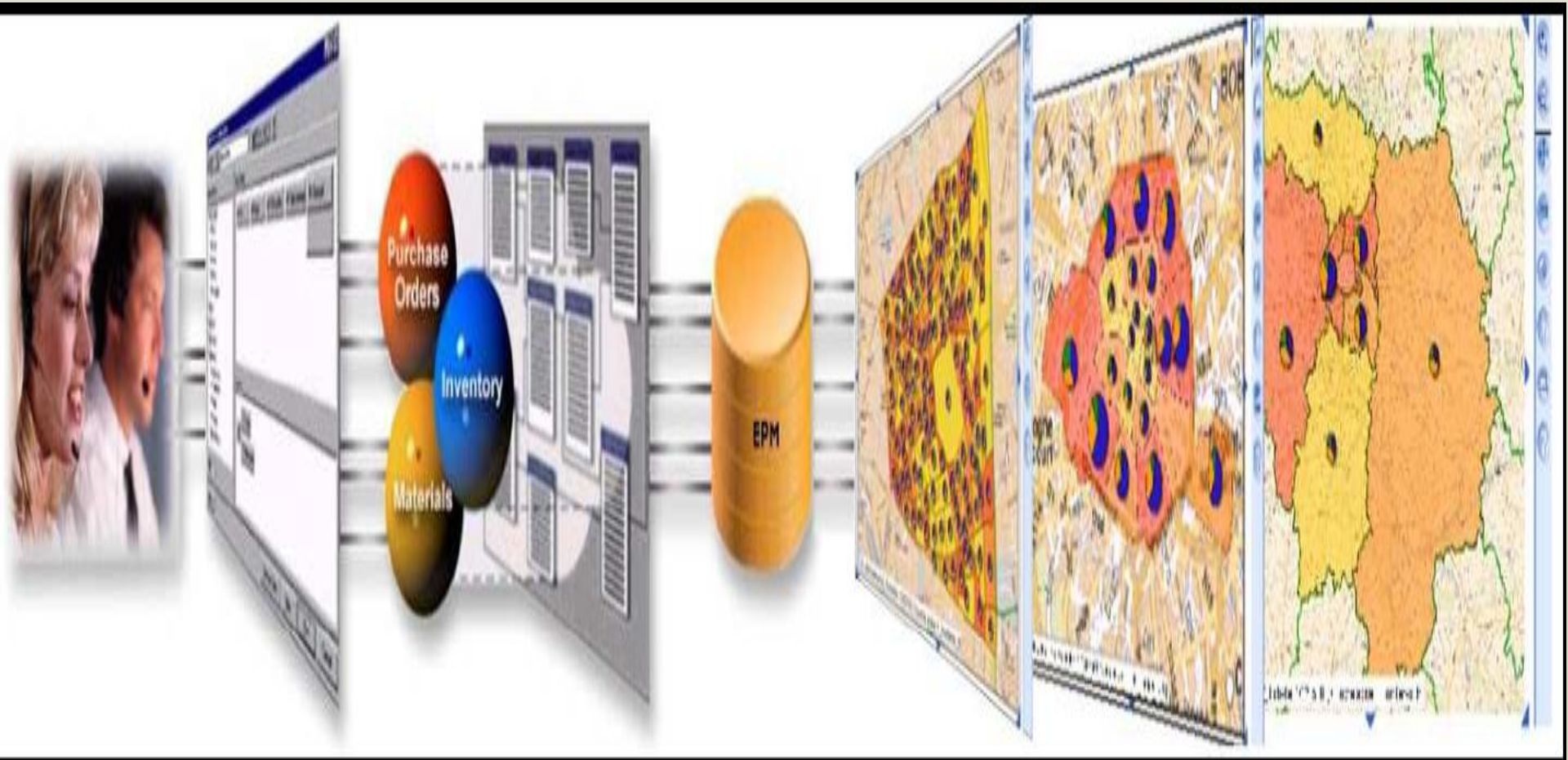
FASODIA Group - ATSYG DECISION - AGROTRANS
E-mail: contact@fasodia.com / Site: www.fasodia.com

INTEGRATEUR DE SOLUTION INFORMATIQUE
Agrément technique: N° ATI-2018-0006
Domaines D5 Catégories: Unique
Arrêté N°201800003/MDENP/SG/DGTIC du 31/01/2018

cisco Select Partner

SEMINAIRE INTERNATIONAL SUR LA PROTECTION DES DONNEES PERSONNELLES

Commission de l'Informatique et des Libertés (CIL) - 10 juillet 2018



Présentation FASODIA Group

Mr. Hamado KINDO
Expert Géodécisionnel

10 BP 614 Ouagadougou 10
BURKINA-FASO

Tel: +226 70 76 28 10

4 Rue Eugene DUPUIS
94000 CRETEIL
FRANCE

Tel: +33 671 117 915

contact@fasodia.com
www.fasodia.com

FASODIA GROUP : Fournisseur de services globaux

FASODIA Group est composé de :

- ATSYG Décision (Europe)
- Agrotrans (Afrique)

FASODIA Group tire profit de son organisation et implantation géographique pour fournir des services complets de premier ordre à ses clients. Ces services incluent souvent:

- Conseil
- Intégration
- Les nouvelles technologies de l'information
- Infogérance
- Intermédiation commerciale

FASODIA Group - ATSYG DECISION - AGROTRANS

FASODIA : Créateur de Systèmes d'informations

Nos spécialités

- Sécurité: des systèmes d'information, Réseau, intranet, Internet (WEB). Certification, horodatage, solutions de Single Sign On (SSO)
- Bureautique et outils de travail collaboratif
- Business intelligence (BI)

  Reporting, ETL, analyse multi-dimensionnelle
- Gestion de la Maintenance Assistée par Ordinateur (GMAO)
- Système d'Information Géographique et Foncier (SIG/SIF)

FASODIA : Créateur de Systèmes d'informations

- Fasodia group est :
  - Intégrateur des suites logiciels ArcGis de ESRI
  - partenaire **Pitney Bowes** sur les solutions MAPINFO
  - partenaire **CISCO** sur les éléments actifs des réseaux informatiques.
- Fasodia group dispose de références significatives:
  - En France: Air France KLM, ERDF, AREVA, EDF,…
  - Au Burkina-Faso: ONEA, SONABEL, Ministère de la Santé, Ministère de l'Agriculture, CCI-BF, Agetib…
- Fasodia group est membre fondateur de l'Ecole Supérieure des Techniques Avancées (ESTA) de Ouaga

Agenda de la présentation

Généralités sur la sécurité des systèmes informatiques

- Introduction
- Système informatique ou système d'information qu'est ce que c'est ?
- Sureté ou sécurité des systèmes informatiques qu'est ce que c'est ?
- Motivations des prédateurs et les risques encourus par des victimes.
- Les causes de vulnérabilités et les moyens pour s'en prémunir.
- Exemple de solution
- Questions

Données, Informations, Connaissances

- **Donnée:**
  - ✓ Décrit des objets ou des événements dignes d ’intérêt.
  - ✓ Ex: La quantité achetée du produit A dans la facture N°6 est de 20 unités.

- **Information:**
  - ✓ Modifie notre vision du monde et réduit l’incertitude. Les données deviennent information par un processus d’interprétation qui fait intervenir les connaissances de l’individu.
  - ✓ Ex: Les ventes du produit A sur la région Nord ont augmenté de 10% en 2012.

- **Connaissance:**
  - ✓ Ensemble de schémas qui augmente notre compréhension (M.J. Earl).
    - ❖ connaissance formalisée ou explicite. Se transmet par le discours. Exemple: le modèle comptable.
    - ❖ connaissance tacite. S’acquiert par la pratique. Exemple: faire du vélo.
  - ✓ Ex: Généralement, un client qui a acheté le produit A achète ensuite le produit B

Information => POUVOIR (1/2)

- **L'Information est source de pouvoir:**
  - ✓ La détention de l'information procure un avantage concurrentiel.
  - ✓ Ex: Un magasin des Etats Unis est devenu leader de son marché en suivant les indications de son système d'information décisionnel qui lui recommandait de **« placer la bière dans les couches culotes des bébés »**

- **La 3ème Guerre Mondiale est celle de l'Information. Elle a commencé à la fin de la 2ème Guerre mondiale entre les alliés:**
  - ✓ Récupération des savants, des médecins, des techniciens Nazis,…
  - ✓ Le **pacte secret UKUSA signé en 1948** (par les Etats-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande) et chapeauté par la National Sécurity Agency (N.S.A) a doté les états membres d'un **réseau mondial d'écoute, de collecte, de traitement et de capitalisation de l'information**. **Echelon, Comint** (captation des ondes) et **ELINT** (surveillance des transmissions) sont des composantes connues de ce réseau dont l'existence a été révélée par un rapport de la Commission d'évaluation des choix technologiques et scientifiques (STOA) de la direction Générale du Parlement Européen

Information => POUVOIR (2/2)

- **Conséquences:**
  - ✓ Marchés remportés par des firmes américaines en écoutant les négociations de la concurrence.
  - ✓ Récemment:
    - Ecoute de la chancelière Allemande
    - Campagne présidentielle USA

- **Développement d'un marché de troc (de dupe pour être plus précis):**
  - ✓ Vos informations contre de petits services:
    - Hébergeurs « dit gratuit »: Google (Gmail, Google Map,…) , Yahoo, Hotmail, etc…
    - Les réseaux sociaux (Twitter, Youtube, Facebook, etc….)
  - ✓ Vos avis pour des prunes:
    - Les Likes
    - Les followers

Conclusion: « Avoir de grandes oreilles et une petite bouche »

Agenda de la présentation

Généralités sur la sécurité des systèmes informatiques

- Introduction
- Système informatique ou système d'information qu'est ce que c'est ?
- Sureté ou sécurité des systèmes informatiques qu'est ce que c'est ?
- Motivations des prédateurs et les risques encourus par des victimes.
- Les causes de vulnérabilités et les moyens pour s'en prémunir.
- Exemple de solution
- Questions

Définitions des systèmes d'information

- **Ensemble de composantes inter-reliées qui recueillent de l'information, la traitent, la stockent et la diffusent afin de soutenir les processus métiers de l'entreprise, la prise de décision et le contrôle au sein de l'organisation.**

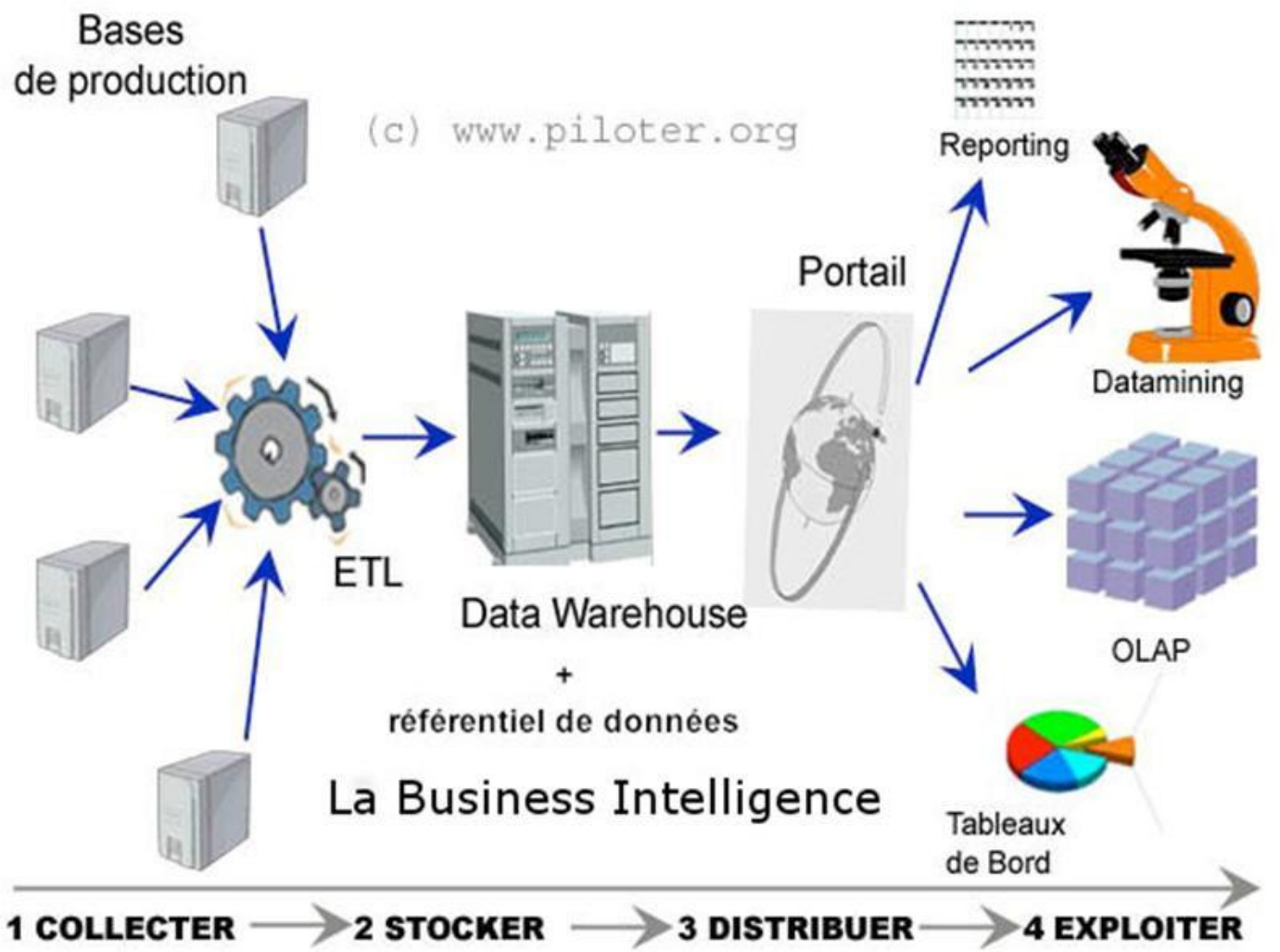
- **Ensemble d'informations nécessaires au fonctionnement de l'entreprise. Ces informations sont internes ou externes, structurées ou non et dont le traitement est automatisé ou non.**

- **C'est un système qui utilise les ordinateurs et les moyens de communication, les procédures manuelles, les référentiels de données internes et externes. Il applique une combinaison d'actions automatiques et humaines ainsi que des interactions homme/machine.**

Conclusion: Le SI sert de support aux processus métiers réalisés par les acteurs dans un cadre organisationnel

Typologie des systèmes d'information

Les fonctions de la chaîne décisionnelle (1/3)



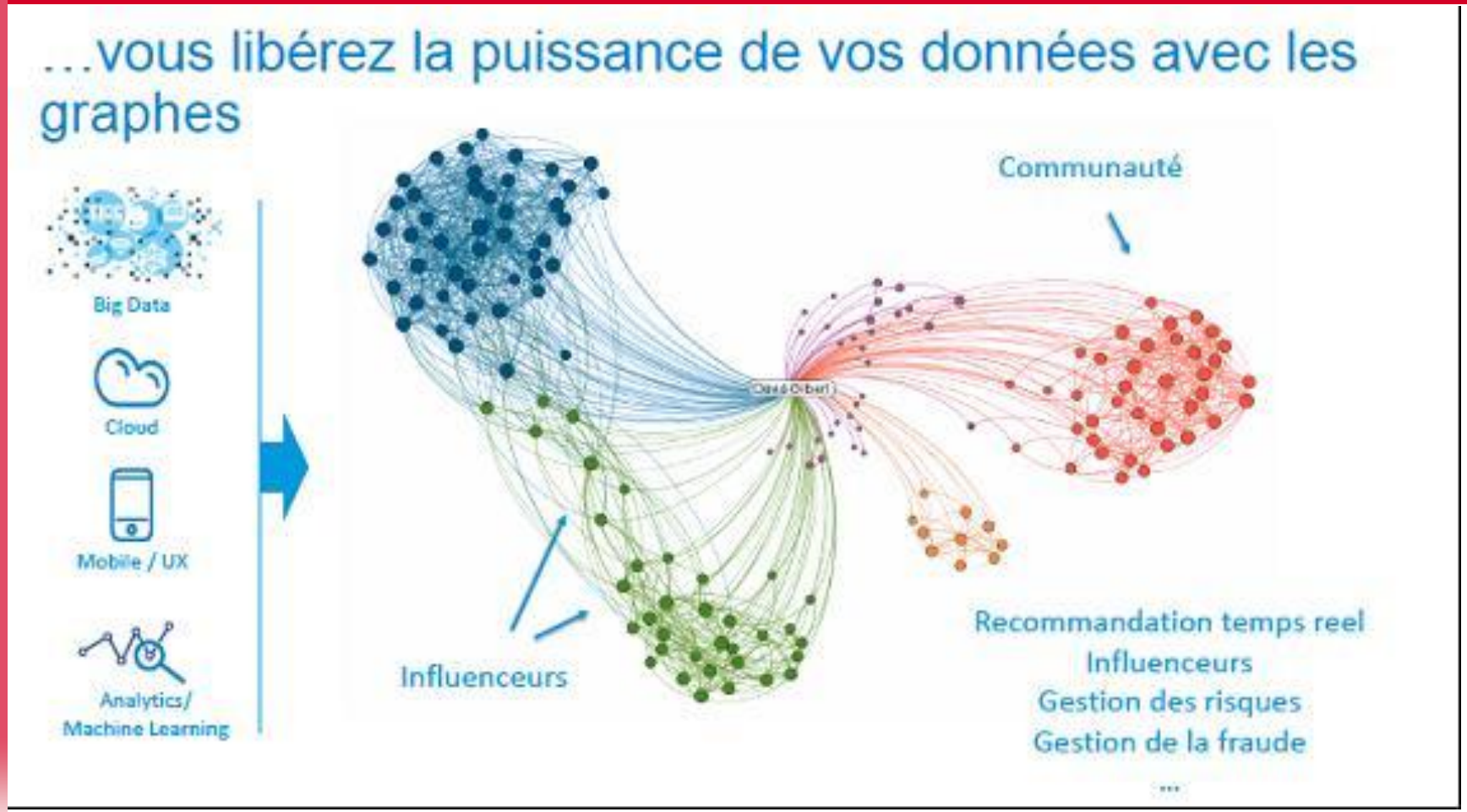
Les fonctions de la chaîne décisionnelle (2/3)

Persistance des données de référence en base graphe

$G=(V,A)$

FASODIA Group - ATSYG DECISION - AGROTRANS

Les fonctions de la chaîne décisionnelle (3/3)



FASODIA Group - ATSYG DECISION - AGROTRANS

La dimension financière

- **Le coût des SI représente entre 5 et 20% du chiffre d'affaires des entreprises ou des frais généraux des organisations.**
- **31% des projets de mise en œuvre de SI sont abandonnés**
- **Seul 13% des projets de mise en œuvre des SI respectent les coûts et délais**

Conclusion: « Le SI est vital. Il faut le protéger et le développer»

Agenda de la présentation

Généralités sur la sécurité des systèmes informatiques

- Introduction
- Système informatique ou système d'information qu'est ce que c'est ?
- Sureté ou sécurité des systèmes informatiques qu'est ce que c'est ?
- Motivations des prédateurs et les risques encourus par des victimes.
- Les causes de vulnérabilités et les moyens pour s'en prémunir.
- Exemple de solution
- Questions

La Sûreté, Sécurité

La sûreté c'est un état, alors que la sécurité, c'est les conditions de protection. On se met en sécurité pour être en sûreté.

La sécurité du SI s'assure que l'entreprise ne risque rien. En somme la sécurité c'est les conditions de la sûreté de la société.

- **Sûreté :**
  - ✓ **Incapacité du système à nuire à son environnement**
  - ✓ **Degré de prévention, de réduction et de réaction approprié vis-à-vis d'un dommage accidentel**
  - ✓ **Un système est critique si sa défaillance est suffisante pour causer un dommage absolu**
- **Sécurité :**
  - ✓ **Incapacité de l'environnement à nuire au système**
  - ✓ **Degré de prévention, de réduction et de réaction approprié vis-à-vis d'un dommage malveillant**
  - ✓ **Un système est critique si sa défaillance est suffisante pour causer un dommage relatif**

La Sûreté, Sécurité

- **Les 5 composantes suivantes du SI doivent être prises en compte dans la mise en œuvre de la sécurité :**
  - ✓ **Le réseau et son équipement**
  - ✓ **Les Systèmes d'exploitation (OS)**
  - ✓ **Les serveurs, les PC, les ordinateurs portables, tablettes, téléphones, etc…**
  - ✓ **Les applications**
  - ✓ **Les utilisateurs**
- **Ces composantes intègrent le matériel utilisé à l'extérieur (domicile par exemple) par les collaborateurs**

Les risques, les causes et les conséquences

- **Les risques**

  Le système d'information est sujet à divers types de risques :

  - ✓ **Intégrité : modification ou suppression de l'information ;**
  - ✓ **Confidentialité : révélation des informations à des tiers (qui ne doivent pas en avoir connaissance) ;**
  - ✓ **Disponibilité : de provoquer des pannes, des erreurs, voire de la malveillance.**

  Certains de ces risques peuvent aussi, directement ou indirectement, causer d'importants dommages :

  - ✓ **Financiers (détournement, vol de N° de carte de crédit...) ;**
  - ✓ **Personnel, causant du tort à la vie privée d'une personne en diffusant des informations confidentielles sur elle;**
  - ✓ **D'image, désinformation, diffamation, permettre à une personne de mettre en évidence des failles de sécurité sur un serveur web…**

Les risques, les causes et les conséquences

- **Causes humaines**

  La maladresse : Erreur humaine. Effacer involontairement des données...

  - ✓ **L'inconscience : de nombreux utilisateurs méconnaissent les risques (mot de passe collé sur l'écran, téléchargement abusifs..**
  - ✓ **La malveillance : une personne qui parvient à s'introduire dans le système, légitimement ou non, peut causer des déguâts.**
  - ✓ **La majeure partie des menaces est due à l'erreur ou la négligence humaine (utilisateurs comme informaticiens).**
  - ✓ **Il ne faut pas les ignorer ou les minimiser.**

- **Causes extérieures**
  - ✓ **Un sinistre (vol, incendie, dégât des eaux)**
  - ✓ **Une malveillance ou une mauvaise manipulation entraînant une perte de matériel et/ou de données.**
  - ✓ **Problèmes électriques (coupures,s urtensions peuvent entrainer la panne des serveurs et disques durs, donc l'accès aux données).**

Les risques, les causes et les conséquences

- **Causes techniques**
  - ✓ **Surchauffe : les processeurs produisent de la chaleur.**
  - ✓ **L'usure : elle est inévitable.**
  - ✓ **Incidents liés au logiciel : des failles permettant de prendre le contrôle total ou partiel d'un ordinateur.**
  - ✓ **.**

Certains de ces risques peuvent aussi, directement ou indirectement, causer d'importants dommages :

- ✓ **Financiers (détournement, vol de N° de carte de crédit...) ;**
- ✓ **Personnel, causant du tort à la vie privée d'une personne en diffusant des informations confidentielles sur elle;**
- ✓ **D'image, désinformation, diffamation, permettre à une personne de mettre en évidence des failles de sécurité sur un serveur web…**

Les typologies d'agression

- **Intrusion**
  - ✓ **Virus**
  - ✓ **Usurpation d'identité**
  - ✓ **C'est le type de problème le plus fréquent**
- **Attaque par déni de service :**
  - ✓ **empêcher le bon fonctionnement d'un ordinateur en saturant le système**
  - ✓ **Problème peu fréquent (« violence gratuite ») mais difficilement évitable**
- **Vol d'informations**
  - ✓ **Par usurpation d'identité (vol actif)**
  - ✓ **Par espionnage (vol passif)**

Les typologies d'agression

- **Les virus**

  Définition : programme situé à l'intérieur d'un autre qui s'exécute pour nuire :

  - ✓ **Simple perturbateur (balle qui traverse l'écran)**
  - ✓ **Détruit les données**
  - ✓ **Se reproduit**
- **Typologie des virus selon leurs objectifs**
  - ✓ **Les espiogiciels (spywares) :**
    - **Collecte des données**
    - **Pour mieux connaître les internautes**
    - **« profilage »**
    - **En général s'installent avec des logiciels libres**
    - **« adwares » = avec la publicité**
  - ✓ **Les enregistreurs de touches (keyloggers) :**
    - **Collecte des données à la source (clavier)**
    - **Même objectif**

Les typologies d'agression

- **Le « spamming » ou postage excessif**
  - ✓ **Publicité à moindre coût**
  - ✓ **Problèmes:**
    - **Largeur de bande, espace disque, personnel, temps perdu,..**
- **Le déni de service**
  - ✓ **Objectif : générer une montée en charge ingérable**
- **Cookies : problème ?**
  - ✓ **Définition :**
    - **fichier contenant des paires clé-valeur permettant à un site de mieux connaître un utilisateur (ou client)**
    - **Concept HTTP**
  - ✓ **Des règles :**
    - **Pas de cookie > à 4Ko**
    - **Pas plus de 300 cookies sur un disque**
    - **Pas plus de 20 cookies créés par un même site**
    - **Tout utilisateur peut interdire la création de ces « cookies »**

Agenda de la présentation

Généralités sur la sécurité des systèmes informatiques

- Introduction
- Système informatique ou système d'information qu'est ce que c'est ?
- Sureté ou sécurité des systèmes informatiques qu'est ce que c'est ?
- Motivations des prédateurs et les risques encourus par des victimes.
- Les causes de vulnérabilités et les moyens pour s'en prémunir.
- Exemple de solution
- Questions

Les typologies des agresseurs

- **Plaisantins : s'amusent**
- **Vandales :**
  - ✓ **cherchent à détruire**
- **Compétiteurs :**
  - ✓ **relèvent des défis**
  - ✓ **collectionnent des exploits**
- **Espions**
- **NB : Hacker < > Cracker**
  - ✓ **le hacker (white hat) cherche à comprendre**
  - ✓ **le cracker (black hat) cherche à nuire**

Agenda de la présentation

Généralités sur la sécurité des systèmes informatiques

- Introduction
- Système informatique ou système d'information qu'est ce que c'est ?
- Sureté ou sécurité des systèmes informatiques qu'est ce que c'est ?
- Motivations des prédateurs et les risques encourus par des victimes.
- Les causes de vulnérabilités et les moyens pour s'en prémunir.
- Exemple de solution
- Questions

Synthèse des menaces

Menaces	Disponibilité	Intégrité	Confidentialité	Traçabilité
écoute du réseau			x	
vol de fichiers			x	
espionnage			x	
ingénierie sociale	x	x	x	x
vers, virus, bombes logiques	x	x		x
spams	x	x		
désinformation		x		
erreurs humaines	x	x		x
pannes	x			x
déni de service	x			x

Les solutions

Menaces	Exemples de contre-mesures
écoute du réseau	cryptographie des données, des communications
vol de fichiers	contrôle d'accès, authentification forte, biométrie
espionnage	classification des actifs
ingénierie sociale	formation du personnel
vers, virus, bombes logiques	antivirus, systèmes de détection d'intrusion
spams	anti-spams
désinformation	formation du personnel
erreurs humaines	politique de sauvegarde, formation du personnel
pannes	politique de sauvegarde, plan de secours informatique
déni de service	pare-feux

Agenda de la présentation

Généralités sur la sécurité des systèmes informatiques

- Introduction
- Système informatique ou système d'information qu'est ce que c'est ?
- Sureté ou sécurité des systèmes informatiques qu'est ce que c'est ?
- Motivations des prédateurs et les risques encourus par des victimes.
- Les causes de vulnérabilités et les moyens pour s'en prémunir.
- Exemple de solution (Recommandations)
- Questions

Méthodologie

- **Conception globale**

La sécurité du SI doit être abordée de façon globale et élaborée au niveau de la DSI :

- ✓ **une "prise de conscience" par les utilisateurs de leurs responsabilités ;**
- ✓ **la sécurité des données ;**
- ✓ **la sécurité réseaux ;**
- ✓ **la sécurité des systèmes d'exploitation (OS).**
- ✓ **La sécurité physique doit aussi être prise en compte, au même titre que la sécurité du matériel, afin d'éviter les sinistres (incendies, vol...).**

- **Mettre en œuvre une politique de sécurité**
  - ✓ **Élaborer des règles et des procédures.**
  - ✓ **Définir les actions à mener et les personnes à contacter.**
  - ✓ **Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'information.**
  - ✓ **Déterminer les rôles et les responsabilités.**

Méthodologie

- **Mettre en œuvre un plan de continuité d'activité (PCA)**

  Exemple par réplication
- **Mettre en œuvre un plan de reprise d'activité (PRA)**

  Exemple par redondance des machines
- **Réaliser une analyse de risque**
  - ✓ **Identifier les menaces : d'origine humaine, naturelle... internes ou externes.**
  - ✓ **Déduire les impacts : pour atténuer les risques.**
- **Réaliser une analyse d'impact**
  - ✓ **C'est-à-dire évaluer un risque, son impact et en déterminer la gravité.**
  - ✓ **Une indisponibilité du site internet institutionnel n'a pas le même degré d'importance que le processus de prise de commande.**
- **Mesurer ces risques en fonction de :**
  - ✓ **la probabilité ;**
  - ✓ **leur fréquence ;**
  - ✓ **leurs impacts.**

Plan d’actions

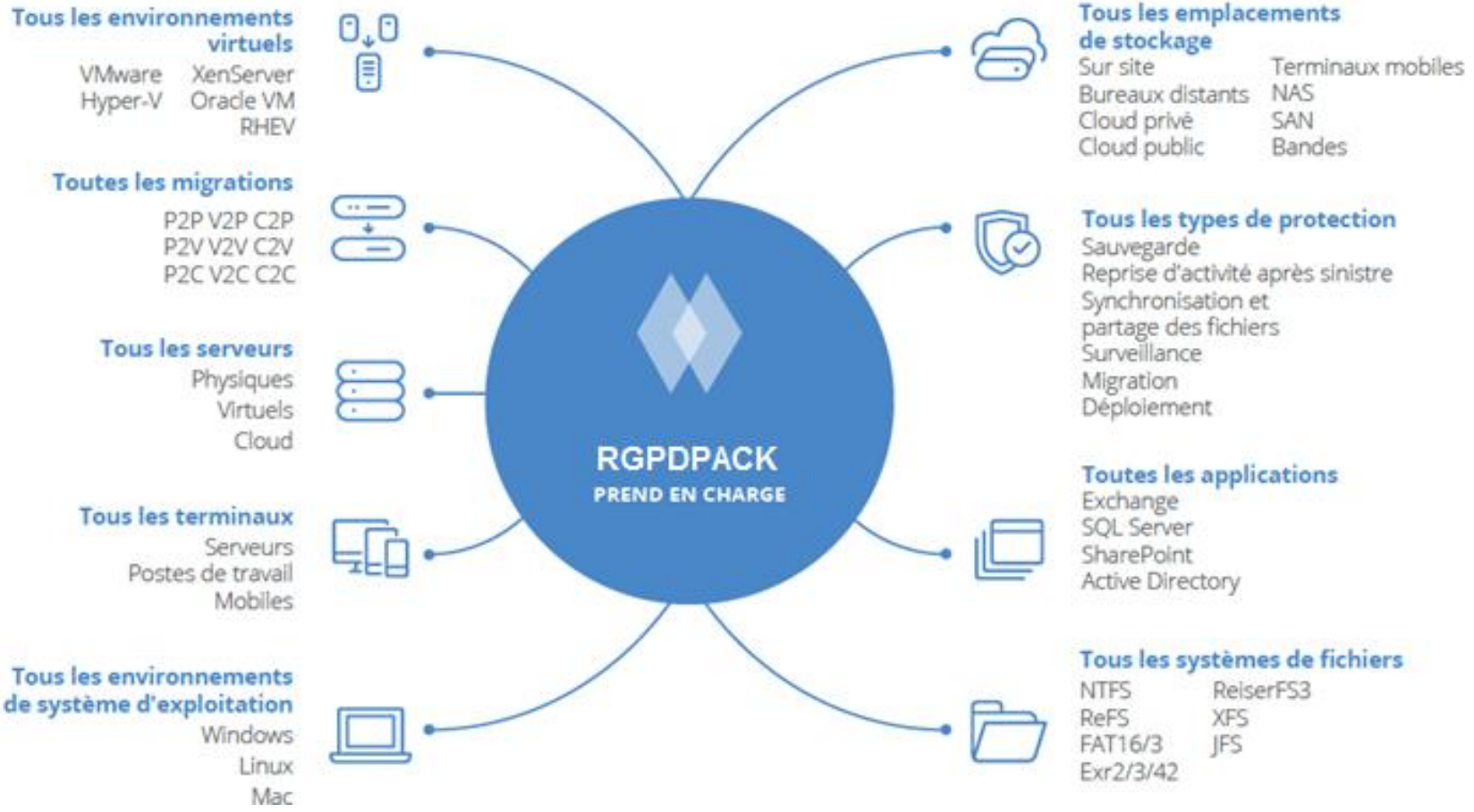
- **Mesures préventives**
  - ✓ **Sensibiliser les utilisateurs.**
  - ✓ **S'assurer de "l'innocuité" des postes de travail et des serveurs.**
  - ✓ **Sécuriser l'accès réseau.**
  - ✓ **Sauvegarder les données.**
  - ✓ **Redondance des matériels : en doublant, on réduit le risque.**
  - ✓ **Dispersion des sites : un accident (incendie, tempête, tremblement de terre, attentat, etc.) a très peu de chance de se produire simultanément en plusieurs endroits distants.**
  - ✓ **Supervision : elle permet de déceler en amont les anomalies.**

- **Mesures curatives**
  - ✓ **La reprise des données : elle doit se faire dans un laps de temps court.**
  - ✓ **Le redémarrage des machines.**
  - ✓ **Le redémarrage des applications.**

Plan d’actions

- **Actions pour les utilisateurs**
  - ✓ **N'utiliser que des applications identifiées.**
  - ✓ **Respecter la confidentialité des codes d'accès.**
  - ✓ **Signaler rapidement les symptômes de panne**
  - ✓ **Etc...**
- **Actions pour les techniciens**
  - ✓ **Connaissance fonctionnelle et technique du système.**
  - ✓ **Sauvegarder régulièrement le SI et s'assurer que ces sauvegardes soient utilisables.**
  - ✓ **Etc...**
- **Actions pour les responsables**
  - ✓ **S'assurer de la validité du plan de reprise d’activité (par exemple valider la mise à jour du système d'exploitation des machine de secours).**
  - ✓ **Etc…**

Les solutions RGPDPACK



Des solutions pour la sécurité de votre SI

Au service de la mise en application de la RGPD

FASODIA Group - ATSYG DECISION - AGROTRANS

Les solutions RGPD

- **Protection complète des données de l'entreprise :**
  - ✓ **21 plates-formes prises en charge.**
  - ✓ **Rôles administratifs.**
  - ✓ **Tableaux de bord personnalisables, alertes intelligentes et rapports.**
  - ✓ **Chiffrement et protection par mots de passe.**
  - ✓ **Options de stockage flexibles : disques locaux, NAS, SAN, lecteurs de bandes.**
- **Prévenir les fuites de données**

  Une solution simple, complète et sécurisée pour l'accès, le partage et la synchronisation de données d'entreprise :
  - ✓ **Solution On-Premise (installée sur site).**
  - ✓ **Cryptage des données.**
  - ✓ **Mécanismes d'authentification forte.**
  - ✓ **Journalisation des actions des administrateurs et utilisateurs.**
  - ✓ **Effacement à distance des données synchronisées.**

Les solutions RGPD

- **Garantir l'authenticité et la non-altération des données et des sauvegardes :**
  - ✓ **S’appuie sur la technologie Blockchain.**
  - ✓ **Génère automatiquement un certificat qui peut être vérifié à tout moment.**
- **Protection active de vos données, contre les rançongiciels et autres menaces par sauvegardes et restaurations instantanées :**
  - ✓ **Protection des données locales et des sauvegardes contre les modifications et cryptages non autorisés.**
  - ✓ **Protection des altérations des sauvegardes Cloud en protégeant l’agent de sauvegarde des attaques.**
  - ✓ **Retour à la normal instantané.**

Conclusion: Les données ne sont jamais compromises.

FASODIA Group - ATSYG DECISION - AGROTRANS
E-mail: contact@fasodia.com / Site: www.fasodia.com

SEMINAIRE INTERNATIONAL SUR LA PROTECTION DES DONNEES PERSONNELLES

Commission de l'Informatique et des Libertés (CIL) - 10 juillet 2018

Merci de votre attention !