3ème année

Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo
RSSI - CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - **Fonctionnement de la sécurité dans une entreprise**
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Environnement de la SSI

- Internes ou associés
  - Service études
  - Service exploitation
  - Sous-traitants
  - Organismes nationaux
  - Tutelles
  - CE/DP
  - Service juridique
- Externes et indépendants
  - Justice
  - ANSSI (www.ssi.gouv.fr)
  - CNIL (www.cnil.fr)
  - CERT/CC (www.cert.org)
    US-CERT (www.us-cert.gov)
    CERTA (www.certa.ssi.gouv.fr)
  - CESTI
  - OCLCTIC
    (http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic)

Organisation dans une entreprise

- Un « responsable » (RSSI)
- Comité de sécurité informatique
- Groupes de travail
  - Mise en place de l'organisation SSI
  - Sensibilisation des utilisateurs
  - Audit et gestion des risques
  - Autorisation et actions de sécurité opérationnelle
  - Surveillance et contrôle
  - Veille technologique
  - *projet*
- Gestion de crise

Fonctions du RSSI

Cigref 2001

- Définition de la politique de sécurité
- Analyse de risques
- Sensibilisation et formation aux enjeux de la sécurité
- Étude des moyens et préconisations
- Audit et contrôle
- Veille technologique et prospective

Rôles de conseil, d'assistance, d'information, de formation et d'alerte.
Si possible indépendant de la direction informatique.

Différents documents

- Analyse des risques
- Politique de sécurité (PSSI)
- Spécifications de sécurité
- Guides de configuration ou de recette sécurité
- Synthèse/Suivi : alertes, filtrage, violations
- Tableau de bord ou audit/contrôle interne

Analyse des risques

1. Identifier les biens et leur valeur
2. Attribuer des priorités aux biens
3. Déterminer la vulnérabilité aux menaces et les dommages potentiels
4. Attribuer des priorités à l'impact des menaces
5. Sélectionner des mesures de protections rentables

Méthodes d'analyse de risques de sécurité

MARION - MELISA - CRAMM - …

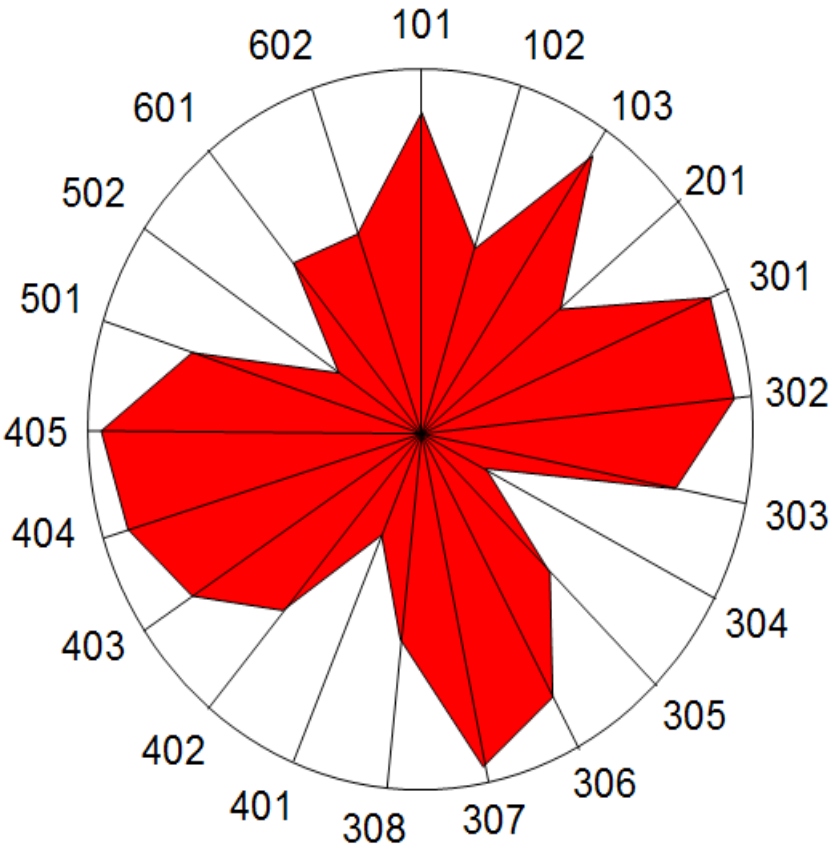
Démarche :

- Identifier les vulnérabilités
- Estimer les menaces (physiques, maladresses, malveillances)
- Analyser les risques et leurs conséquences possibles
- Évaluer les coûts des dégâts correspondants
- Calculer les fréquences*coûts
- Évaluer les coûts des contre-mesures
- Implémenter les plus rentables
- Suivre l'évolution

Indicateurs (Marion)

- Répartis en 6 thèmes
  - la sécurité organisationnelle
  - la sécurité physique
  - la continuité de service
  - l'organisation informatique
  - la sécurité logique et l'exploitation
  - la sécurité des applications
- Face à 17 types de menaces

  Accidents physiques, Malveillance physique, Panne du SI, Carence de personnel, Carence de prestataire, Interruption de fonctionnement du réseau, Erreur de saisie, Erreur de transmission, Erreur d'exploitation, Erreur de conception / développement, Vice caché d'un progiciel, Détournement de fonds, Détournement de biens, Copie illicite de logiciels, Indiscrétion / détournement d'information, Sabotage immatériel, Attaque logique du réseau



Méthodologies de sécurité

- Vont au-delà de l'évaluation des risques : MARION -> MEHARI, OCTAVE
  - ANSSI : EBIOS (expression des besoins et identification des objectifs de sécurité)
  - ISO 27000 : Système de Management de la Sécurité de l'Information (SMSI)
    <http://www.iso27001security.com/html/iso27000.html>
    - 27000 : Vue d'ensemble et vocabulaire (publié en 2009)
    - 27001 : Exigences (2005)
    - 27002 : Code de bonnes pratiques pour le SMSI (2005, anciennement ISO 17799)
    - 27003 : Lignes directrices pour la mise en œuvre du SMSI (publié en 2010)
    - 27004 : SMSI — Mesurage (publié en 2009)
    - 27005 : Gestion des risques en sécurité de l'information (publié en 2008)
    - 27006 : Exigences pour les organismes d'audit et de certification (publié en 2007)
    - 27007 : Lignes directrices pour l'audit des SMSI (publié en 2011)
    - 27008 : Lignes directrices pour le management de la sécurité de l'information (2011)
    - 27010 : SMSI inter-organisationnel (publié en 2012)
    - 27011 : Guide pour les organisations de télécommunications (publié en 2008)
    - 27031 : Lignes directrices … pour continuité des affaires (publié en 2011)
    - 27032 : Cybersécurité (2012)
    - 27033 : Sécurité de réseau (parties 27033-1 à 3 publiées)
    - 27034 : Sécurité des applications (27034-1 publiée en 2011)
    - 27035 : Gestion des incidents de sécurité de l'information (2011)
    - 27799 : SMSI pour le domaine de la santé, basé sur 27002 (publié en 2008)

Pros (my view)

- *Identification* of assets and their relative values
- Assets value offers an opportunity to budget realistically (for protection)
- Is understandable by end users
  - Quite easier than assembly language exploits or cryptographic hash functions
- Risk management alternatives
  - Transfer (insurance, state, etc.)
  - Acceptance (life is deadly after all)
  - Reduction (work, work, work, work, ...)
  - Avoidance (just do it the other way)
- Management could express clear priorities

Cons (my view)

- Threat determination is an oracle problem
- May be used to demonstrate that (any) risk is (already) managed
  - Some forgotten successes of risk management
    - Lehman-Brothers financial risk exposure
    - Greek debt control
  - Qualitative also means manipulable
- Relies a lot on best practices or risks lists
  - Fuels paranoia and ready-made useless tools
  - Does not help target real assets
- Management rarely wants to decide
- Sometimes does not end well morally speaking
  - For example : product lifetime optimization
    (NB : Inherently viewpoint-based)

(Le point de vue d'un informaticien incompétent en matière de droit sur la) Législation

- La protection des informations nominatives est forte et obligatoire en France (CNIL)
- L'utilisation du chiffrement est sujette à contrôle strict en France (DCSSI)
- Toutes les législations et conventions s'appliquent (au système d'information)
  - Lois, décrets, ordonnances, circulaires, …
  - Secret médical, secret bancaire, secret professionnel, …
  - Droit du travail, convention collectives, règlements intérieurs
  - Droit commercial, contrats, …
  - …
- La signature numérique est en attente de jurisprudence
- La preuve numérique également

  (Si, aprés MD5, SHA-1 tombe aussi, l'attente pourrait durer...)

Les actions concrètes du RSSI

- www.cert.org, www.us-cert.gov, www.certa.ssi.gouv.fr
- Paramétrage du *firewall*
- Animation du comité de sécurité et des groupes de travail
- Documentation (PSSI, guides, etc.)
- Interaction avec les organismes extérieurs

- Suivi des tests d'intrusion, gestion des autorisations

Traitement du risque ou simple gestion ?

L'Agence Nationale de la Sécurité des Systèmes d'Information (depuis 2011)

Des évolutions intéressantes:
http://www.ssi.gouv.fr/fr/anssi/publications/discours-de-patrick-pailloux-lors-de-la-conference-de-cloture-des-assises-de-la.html (lien local)

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - **Définition d'un schéma directeur sécurité**
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés
  - Principes de conception et d'utilisation

Schéma directeur SSI

- Ensemble documentaire constitué par
  - PSSI (Politique de sécurité du syst. d'info.)
  - Spécifications ou règlements de sécurité par domaine
    - réseau, système, SGBD, développement, marchés, etc...
  - Guides pratiques et/ou points de validation
    - AIX 5.x, W2K Server SP4, IOS 12.x, Apache 1.2, etc.
  - Dossiers de sécurité des applications
    - paye, achats, compta., métier 1, métier 2, etc.
  - Gestion des risques (audit, suivi)
  - Tableau de bord
  - Plan d'action

PSSI

- Structure
  - Organisation et responsabilités
  - Intégration et interactions de la SSI
    - SSI et projets
    - SSI et exploitation
  - Objectifs de sécurité de l'organisme
  - Règles générales de sécurité
  - Gestion des risques

Modèle de PSSI diffusé par la DCSSI

- Domaines d'application
  - Communications
  - Violations
  - Vie privée
  - Achats de matériels
  - Messagerie
  - Maintenance
  - Audit
  - Communications
  - Identification
  - Authentification
  - Surveillance
  - Contrôle d'accès
  - Disponibilité
  - Réseau
  - …

Caractéristiques d'une bonne PSSI

- Réaliste
- Applicable
- Vision à long terme
- Clarté et concision
- Basée sur des rôles ou des profils
- Définition claire des domaines de responsabilité et d'autorité
- À jour (revue périodiquement)
- Communiquée à tout le personnel

« Spécifications »

- Spécifications de sécurité
  - Clauses contractuelles
  - Charte déontologique et utilisateurs (finaux, administrateurs, etc.)
  - Composants réseau
  - Systèmes
  - Collecte des traces et « cybersurveillance »
  - Systèmes d'authentification
  - Application (*X*, *Y*, *Y*, etc.)
  - Données (*A*, *B*, *C*, *D*, etc.)

Documents opérationnels

- Guides de configuration / Points de contrôles
- Déclinés précisément par :
  - Système d'exploitation
    SunOS 4, AIX 4, 5, Solaris 2.6, 2.7, 2.9, RedHat 6, 7, Debian 2.2, 3.0, OpenBSD 3.3, 3.4, etc.
  - Logiciel
    iPlanet, Apache 1.3, 2, IIS 4, 5, 6, etc.
  - Equipement
    Routeurs Cisco 36xx, Nortell 2430, 5430
- Couvre des éléments de configuration ou de vérification concrets

```
echo "0" > /proc/sys/net/ipv4/ip_forward                    Linux procfs
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
net.inet.ip.forwarding=0                                    (Open)BSD sysctl(.conf)
vm.swapencrypt.enable=1
```

Face au cycle de vie d'un projet

- Besoin détaillé ? → Prendre en compte la PSSI
- Étude ? → Spécifications sécurité
- Appel d'offres → Spécifications sécurité
- Développement
- Intégration
- Validation
- Exploitation → Configuration / Contrôle sécurité
- Maintenance → Suivi / Surveillance
- Démantèlement ? → Quid ?

Petit tuyau: www.dban.org
(Darik's Boot And Nuke)

Positionnement par rapport aux différents projets des entreprises

- Projets SSI
  - Associés à l'infrastructure de sécurité elle-même
  - Jonction avec les autres projets d'infrastructure
- Assistance aux projets
  - Apporter des compétences
  - Intégrer la démarche sécurité aux projets
  - Clauses contractuelles
- Validation et contrôle des projets
  - Identifier des vulnérabilités et des risques résiduels
  - Accorder des autorisations d'ouverture

Veille, Suivi

- Veille technologique
  - Alertes CERT (cf ci-avant)
  - Alertes des constructeurs
  - Nouvelles vulnérabilités
  - Nouvelles techniques de protection
- Suivi de la sécurité
  - Contrôles réguliers des vulnérabilités
  - Suivi des préconisations
  - Validation de certaines configurations (e.g.: présence des antivirus)

Synthèse – Tableau de bord

- Rendre compte
  - de la mise en place des règles
  - de l'efficacité des mécanismes de sécurité (et de leur rentabilité)
  - du niveau de vulnérabilité et de risque
  - des agressions
- Évaluer le niveau de maturité