Veille Alerte Réponse
Le Centre Opérationnel en SSI

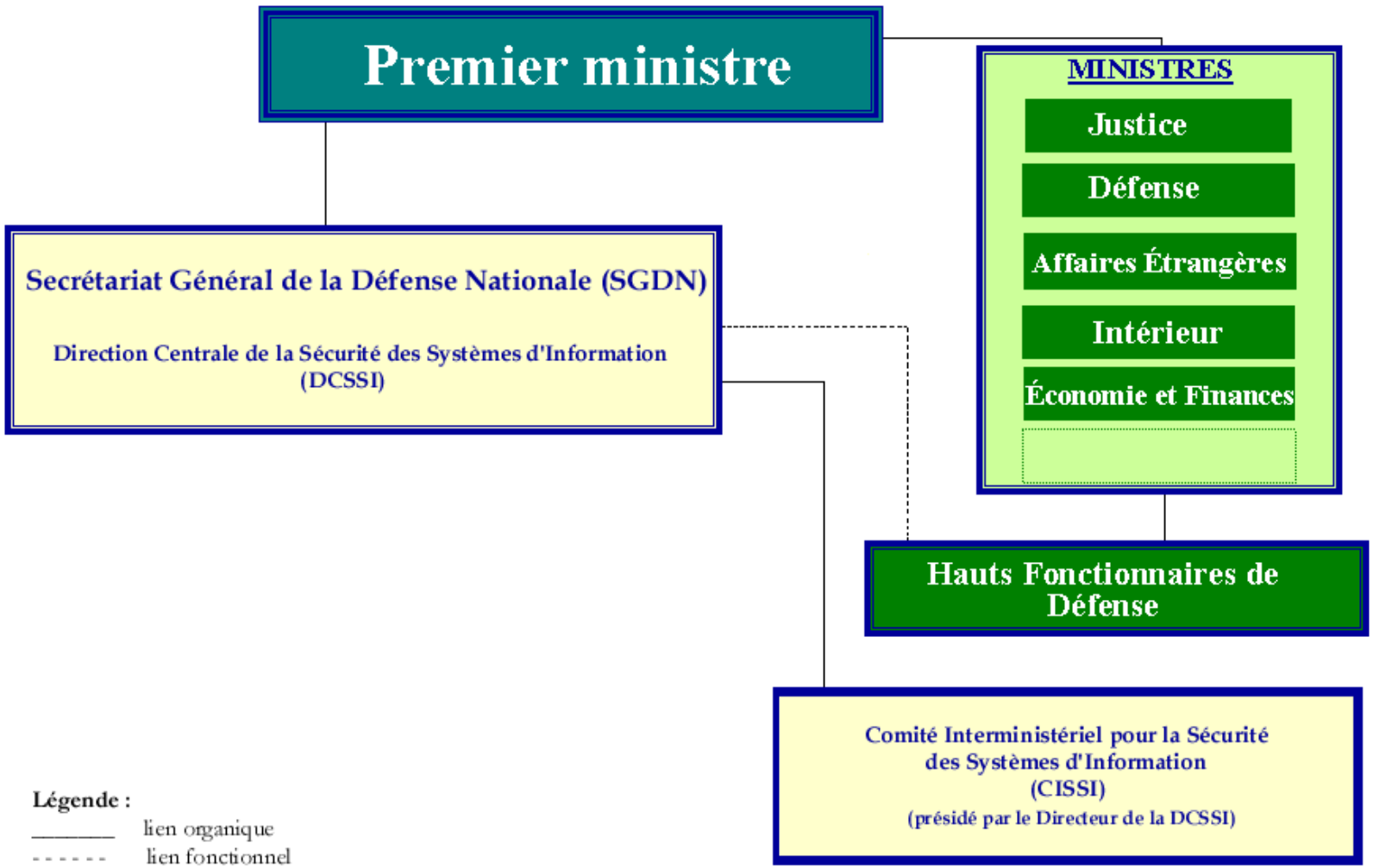
OSSIR - 11 septembre 2006

Stanislas de Maupeou
maupeou@certa.ssi.gouv.fr

Plan

- Le centre opérationnel de la SSI : COSSI
- Une équipe de traitement d'incident : le CERTA
- Le traitement d'incidents: constats et recommandations

L’ organisation de la SSI en France



Le COSSI - Historique

- Date de création : 2003, dans le cadre des plans de vigilance et d'intervention (Vigipirate et Piranet).

- Mission : assurer la coordination interministérielle de prévention et de protection contre les attaques informatiques au profit des autorités gouvernementales.

- Régime permanent (24x7) depuis le 16 mai 2005.

- D'abord tourné vers les attaques terroristes, le COSSI a logiquement évolué vers une prise en compte générique des incidents

Organisation du COSSI

COSSI

Unité Conduite & Synthèse : CEVECS

Unité Technique et Intervention : CERTA

Conduite opérationnelle
Conduite préventive

- Conseil
- Pilotage
- (Mise en garde, Alertes, déclt…)
- Exercices

Veille 24/24 7/7

- Information
- Prévention
- Protection
- Alerte

Ministères

Partenaires

- FIRST
- TF-CSIRT
- CERT gouvernementaux
- CERT français
- Sources ouvertes spécialisées
- Traitement d'incident

La veille 24/24 - Objectifs

1. **Prévention** : apporter les éléments nécessaires pour faire face à des attaques possibles (menaces potentielles)
2. **Alerte** : sur incidents détectés ou prévisibles
3. **Protection** : apporter les éléments nécessaires pour faire face à une attaque déjà débutée
4. **Information** : permettre de diffuser des informations de portée générale

La veille 24/24 - Sources

Quatre types de sources :

1. **Sources ouvertes** : médiatiques, spécialisées dans le domaine SSI ou expertes
2. **Sources fermées** : services de renseignements, services spécialisés en criminalité informatique

3. **Sources intermédiaires** : réseaux de CERTs (français, européens ou internationaux)
4. **Sources opérationnelles** : remontée des «clients» vers le COSSI ou analyse directe d'évènements (journaux de pare-feux, de sondes, …)

La veille 24/24 - Principes

- **Veille de jour** réalisée par des techniciens avec présence d'ingénieurs experts [CERTA] en soutien si nécessaire [interprétation/décision]
- **Veille de nuit** réalisée par des ingénieurs avec le soutien de personnels en astreinte à domicile
- A tout moment 4 personnes au minimum sont rapidement mobilisables au COSSI
- Importance des corrélations entre les différentes veilles

La veille 24/24 – Conduite de crise

- Personnels formés à la conduite de crise [actions qui suivent directement la détection ou la prise en compte d'un incident]
- Aide à la déclinaison des plans auprès des maîtrises d'ouvrage
- Exercices périodiques
- Moyens de communications opérationnels redondants et maîtrisés

Plan

- Le centre opérationnel de la SSI : COSSI
- Une équipe de traitement d'incident : le CERTA
- Le traitement d'incidents: constats et recommandations

Le CERTA

- Création du CERTA par décision du Comité Interministériel pour la Société de l'Information (CISI) du 19 janvier 1999

- L'équipe du CERTA est opérationnelle depuis décembre 1999.

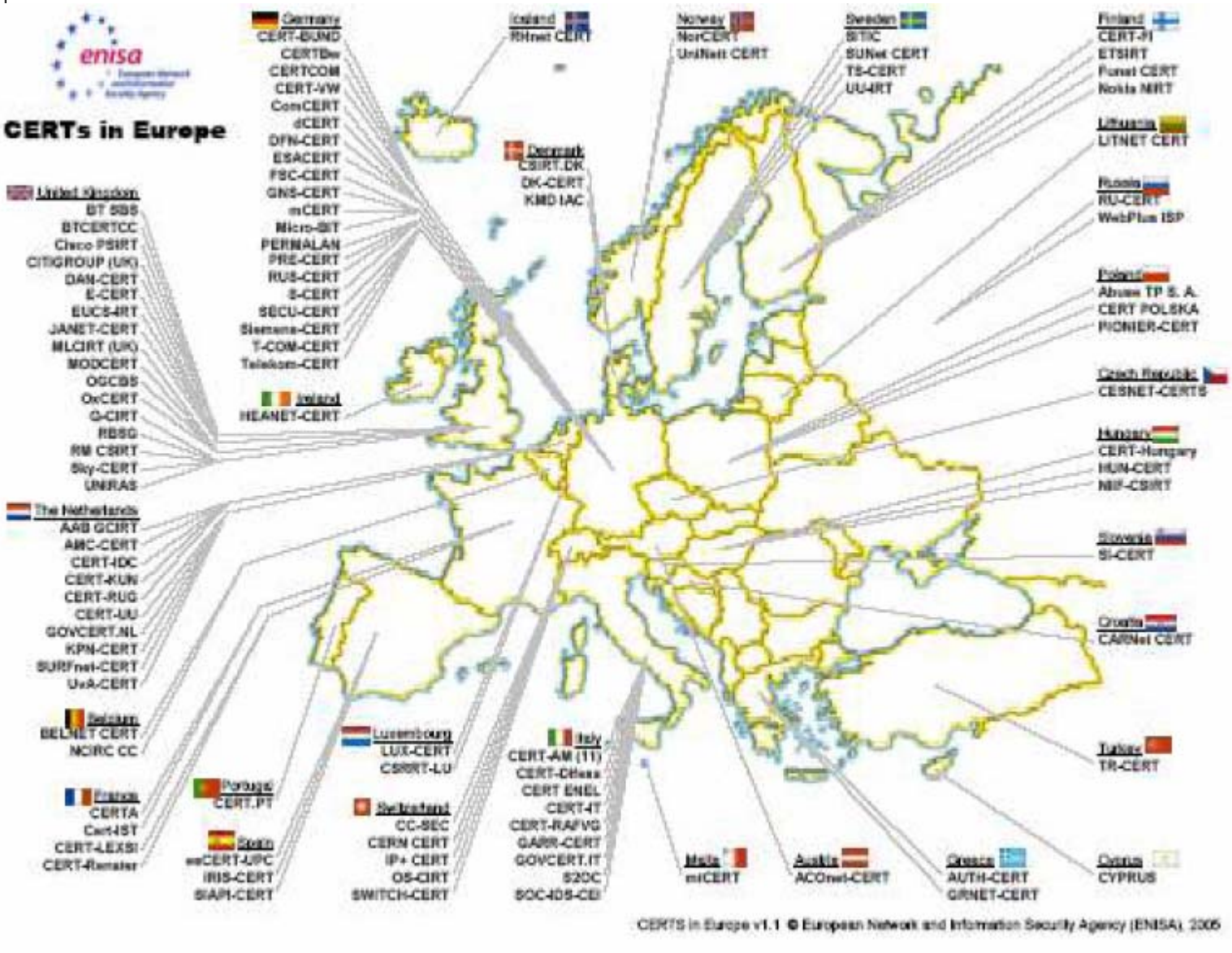
- L'intégration du CERTA dans les réseaux mondiaux de CERTs s'est faite très rapidement : adhésion au FIRST en 2000 et accréditation par le Trusted Introducer en 2001.

- Le CERTA fait partie du centre opérationnel en SSI (COSSI)

Les CERTs en France

- Quatre CERTs en France (membres du FIRST et/ou TF-CSIRT) :
  - ***CERTA*** (*Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques*)
  - ***CERT-IST*** (Industrie Services et Tertiaire), CSIRT commercial créé fin 1998, (quatre partenaires: ALCATEL, CNES, ELF et France Télécom)
  - ***CERT-RENATER***, partie du GIP RENATER (réseau académique) (*Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche*)
  - ***LEXSI***, CSIRT commercial

Premier ministre

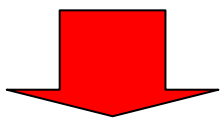


L’assistance opérationnelle du CERTA

Rôle préventif

Fourniture de documents

a priori

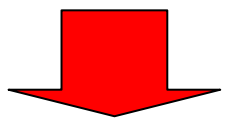


L’aide à la décision pour le RSSI

Rôle curatif

Analyse et intervention

a posteriori



La réponse technique à l’incident

Le rôle préventif du CERTA

Le CERTA distribue des informations nécessaires à la protections des systèmes d'information :

- envoi direct dans les ministères
- diffusion sur le web : http://www.certa.ssi.gouv.fr
- documents synthétiques, pragmatiques et en français

Plus de 2000 documents maintenus à jour :

- **AVIS** : brève description de la vulnérabilité et moyens de s'en protéger
- **ALERTES** : *avis* pour lesquels le moyen de se protéger n'a pas encore été publié ou qui demandent à être traités en urgence.
- **NOTES D'INFORMATION** : plus documentées que les simples *avis* ou *alertes*, elles donnent une explication complète d'un mécanisme.
- **RECOMMANDATIONS** : concernent plus particulièrement des mesures et des méthodes d'organisation.
- **BULLETINS D'ACTUALITE** sont un aperçu hebdomadaire de l'activité vue par le CERTA.

Le rôle curatif du CERTA

- Points clefs dans la résolution d'incidents :
  - prévenir le CERTA d'un incident dès sa détection ;
  - ne pas attendre d'être débordé ;
  - une machine compromise l'est souvent depuis longtemps …;
  - les mises à jour sont souvent l'excuse facile à un incident…;
  - capitaliser (retour d'expérience) à la suite d'un incident.

- Le CERTA : un savoir-faire dans la gestion des incidents
  - ✓ expertise technique reconnue ;
  - ✓ procédure d'intervention adaptée ;
  - ✓ réseaux de confiance indispensables ;
  - ✓ mutualisation des savoirs-faire.

Les services rendus par le CERTA

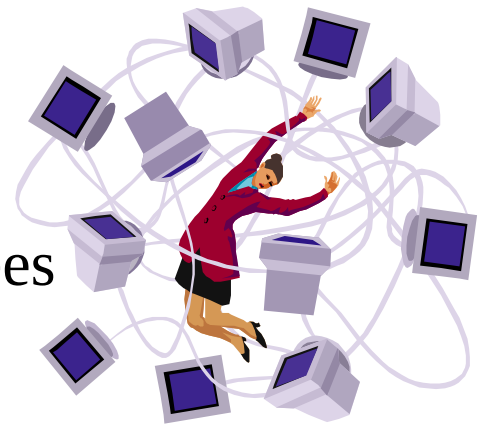
- **Prévention**
  - ✓ analyse ou aide à l'analyse des journaux
  - ✓ veille et publications sur les vulnérabilités
  - ✓ estimation de certaines tendances
  - ✓ maintien d'un niveau de vigilance
  - ✓ aide à la décision pour les RSSI
- **Intervention**
  - ✓ analyser une attaque
  - ✓ proposer des parades

Plan

- Le centre opérationnel de la SSI : COSSI
- Une équipe de traitement d'incident : le CERTA
- Le traitement d'incidents: constats et recommandations

Périmètre du SI…

- L'espace dans lequel s'applique ma(s) politique de sécurité(s)
- La notion de système fermé n'a plus beaucoup de sens
  - ✓ besoin d'échanges toujours plus rapide et facile
  - ✓ télémaintenance et infogérance
  - ✓ partenaires, sous-traitants, etc.
- Les interconnexions maîtrisées, subies ou cachées
  - ✓ passerelles spécifiées et auditées
  - ✓ poids de la sécurité et exigences métiers…
  - ✓ les supports amovibles, les téléphones, les PDA….
- La convergence telecom/informatique :
  - ✓ la disponibilité parent pauvre de la sécurité informatique
  - ✓ la disponibilité exigence fonctionnelle des télécoms

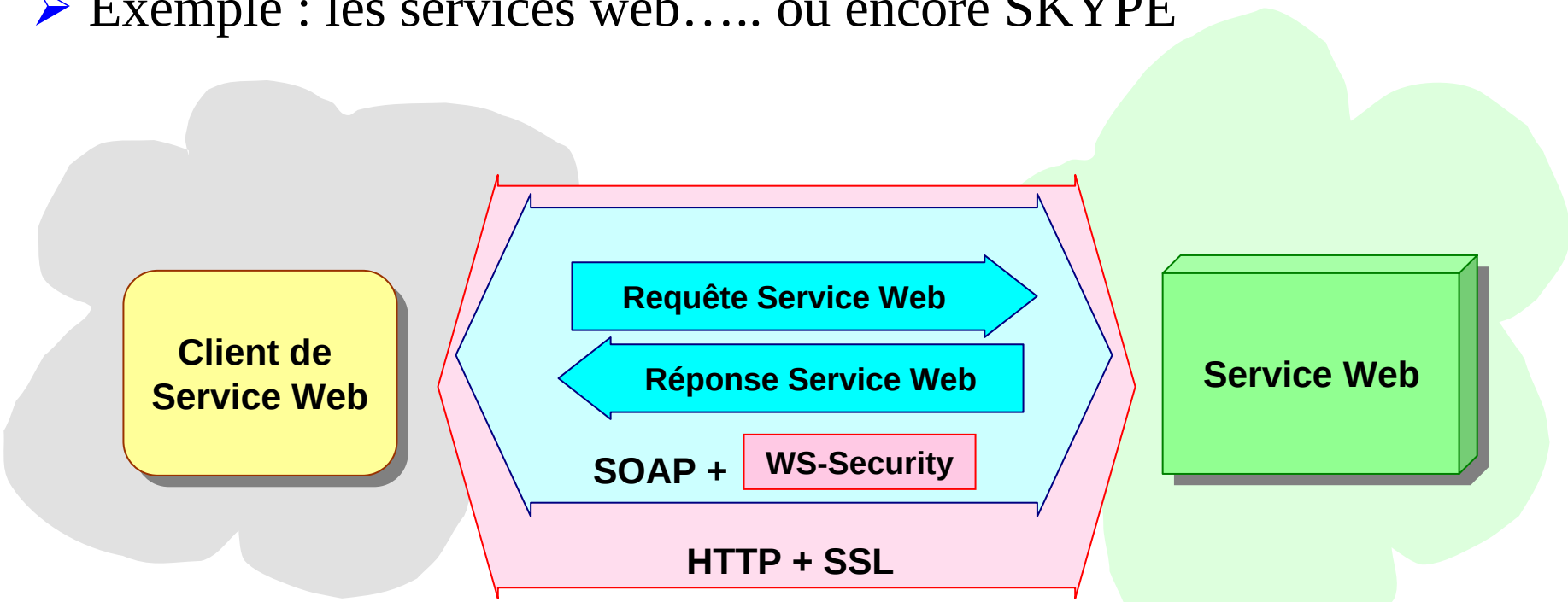


Périmètre du SI…

- Aporie de la gestion des mises à jour et de l'hétérogénéité des parcs
- L'utilisateur est à la fois au cœur et à la limite du périmètre
  - ✓ la couche humaine du modèle ISO
  - ✓ équipements personnels
  - ✓ gestion de la mobilité (accès à distance, réseaux sans fils)
- Le co-hébergement ou la susceptibilité aux attaques indirectes
- Le temps des achats de nouveaux logiciels et le temps de leur maîtrise
- La course vers plus de fonctionnalités cache la complexité de la sécurité

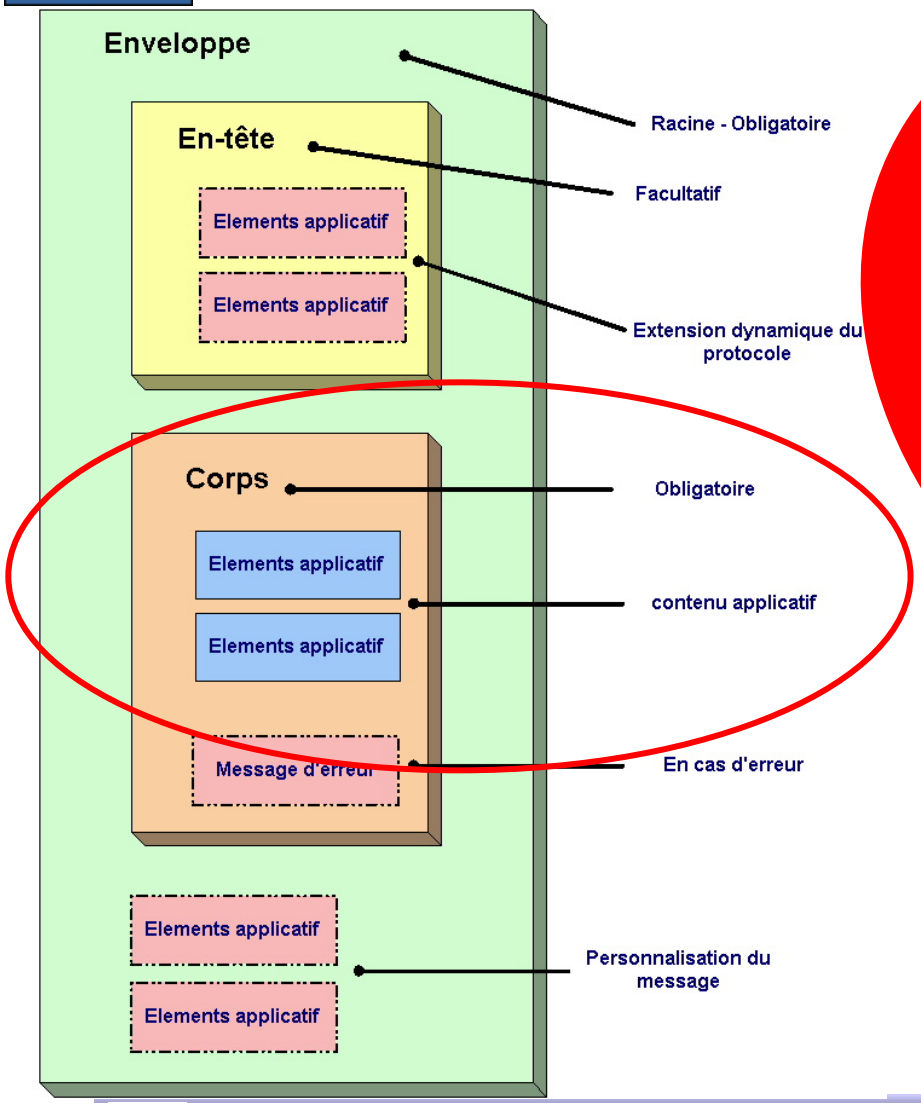
Périmètre du SI…

- Tunnel HTTP et Firewall : une cohabitation difficile…
  - ✓ attention à l'illusion du firewall comme redoute définissant le périmètre
  - ✓ les tunnels HTTP ou HTTPS ont pour but de contourner les firewall
- Exemple : les services web….. ou encore SKYPE



SOAP est le canal standard d'échange des requêtes / réponses des Services Web

Enveloppe SOAP



Il devient donc possible d'encapsuler des protocoles interdits par la politique de sécurité sur HTTP ou HTTPS.

Périmètre du SI : du constat aux recommandations….

- Co-hébergement et effets de bord :

http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005

- Journaliser et analyser….
  - ✓ une barrière doit être vérifiée
  - ✓ le CERTA peut vous aider
- Prendre en compte la complexité de la mobilité (connexion intermittentes à différents réseaux maîtrisés ou non) :
  - ✓ authentification des utilisateurs
  - ✓ protection en confidentialité des données

Périmètre du SI : du constat aux recommandations….

- Gestion des mises à jour : réaction et responsabilité du RSSI lors de la réception d'un avis ou d'une alerte
  - ✓ les systèmes obsolètes : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003
- Sensibiliser les utilisateurs
  - ✓ que faire en cas d'intrusion : http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002
  - ✓ la qualité des mots de passe : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001
  - ✓ Les virus : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002
- Problématique des tunnels
  - ✓ Tunnel et pare feux une cohabitation difficile :

http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003 révision du 5 octobre 2005

Vulnérabilités

- Au sens d'EBIOS, une vulnérabilité est une caractéristique du SI que l'élément menaçant exploite pour conduire son attaque
- Aucun logiciel n'échappe à des bogues
- Une vulnérabilité peut être technique et/ou organisationnelle
  - ✓ bogue logiciel ayant un impact sur la sécurité
  - ✓ absence de politique antivirale
- Dans l'appréciation d'application d'un correctif, le RSSI prend en compte les vulnérabilités à exploiter pour conduire l'attaque (et donc des barrières à faire tomber)
  - ✓ installation d'un cheval de Troie exigeant un clic malheureux de l'utilisateur
  - ✓ installation d'un cheval de Troie sans action préalable de l'utilisateur

L'économie des vulnérabilités…..

- Vulnérabilités et codes permettant leur exploitation se monnayent
- La cybercriminalité exploite les vulnérabilités : phishing; spam; spyware ..

L'éthique des CERTs interdit de publier des codes exploitant des vulnérabilités

- Inventaire des applications du SI
- S'appuyer sur un CERT pour maintenir un niveau de vigilance
- Appliquer les correctifs au cas par cas (coût)
- Gérer l'application d'un correctif dans une approche de défense en profondeur et de gestion des risques

Ce que l'on observe…

Ce que l'on traite

✓ **Attaque sur les mots de passe faibles**: compromission de machines et prise de contrôle à distance avec tous les droits

✓ **Défigurations de sites :** atteinte à l'image et attaque voilée

✓ **Réseaux sans fil non sécurisés** : intrusion sur les réseaux

✓ **Attaque par chevaux de Troie** : vol d'informations sensibles ou confidentielles comme par exemple avec des « keylogger »

✓ **Réseaux de machines compromises** pouvant conduire à des attaques coordonnées (BotNet)

Comment se protéger ?

➢Messagerie instantanée (publication en 2001)

➢« Cross Site Scripting » (2001)

➢Réseaux sans fil (2002)

➢Sécurité des applications web (2004)

➢Attaque ciblée par cheval de Troie (2005)

➢Les mots de passe (2005)

➢Le filtrage (2006)

➢IPV6 (en préparation)

Conclusion sous forme de constat: les CERTs sont une aide à la décision …

- **Les attaques réussies sont des attaques surprises :** l'expérience des CERT permet d'atténuer l'inévitable panique.
- Quand l'attaque est **visible le mal est déjà fait**…mais traiter les conséquences n'est pas suffisant! Les CERTs vous aident à comprendre les causes.
- Beaucoup de bruit pour rien et des attaques furtives, cachées. Presse et effet loupe : les CERTs apportent une certaine rationalité.
- Le temps de la maturité et le temps du déploiement de nouvelles fonctionnalités: gestion des capacités, suivi des correctifs et suivi des parcs.
- Gestion des risques. «*L'incident est rare donc il ne m'arrivera pas*» : la recherche du meilleur coût a un prix!
- **La force des CERTs et leurs limites** : la gestion de la communication et l'impact des mesures correctives échappent souvent aux capacités des CERTs

Conclusion sous forme de recommandations

- Mesurer et tester sa capacité de travail en mode dégradé.
- Anticiper l'impact des risques nouveaux (Google Desktop, offre de stockage gratuit, ToIP, IpV6, BDE, etc.)
- Politique de mise à jour: connaître son parc et se doter d'une capacité et d'une légitimité pour appliquer un correctif
- Distribuer la vigilance : attention aux agressions spécifiques ou de basse intensité (risque de passer inaperçu). Équilibre technique/**organisation**.
- Faire appel à des professionnels pour estimer le niveau de protection et traiter les incidents.

Conclusion

- La France s'est dotée d'une capacité de « veille alerte réponse » opérationnelle
- Le besoin d'information vers les PME et le grand public sur les aspects de sécurité des systèmes d'information
- Il faut former les administrateurs dans la réaction face à un incident
- Le traitement d'incident requiert une forte expertise
- La capacité de « veille alerte réponse » est une composante essentielle de la politique de sécurité

http://www.certa.ssi.gouv.fr