Menaces sur les systèmes d'information

- **Un environnement propice**

Une dépendance accrue

Une diffusion des savoirs pour des acteurs plus nombreux

Une nécessaire dynamique pour la sécurité des systèmes d'information

Les années 70-80 (événements indicatifs)

Naissance de l'Internet : Réseau nodal de transmission conçu comme une réponse à une problématique militaire de continuité d'acheminement de l'information numérique

Prise de conscience du besoin de sécurité : méthodes d'analyse du risque informatique (Marion, Melisa en France)... et naissance du Chaos Computer Club de Hambourg.

Evolution des architectures informatiques

Décentralisation : du terminal-hôte au client-serveur

Distribution : les données brutes deviennent des informations

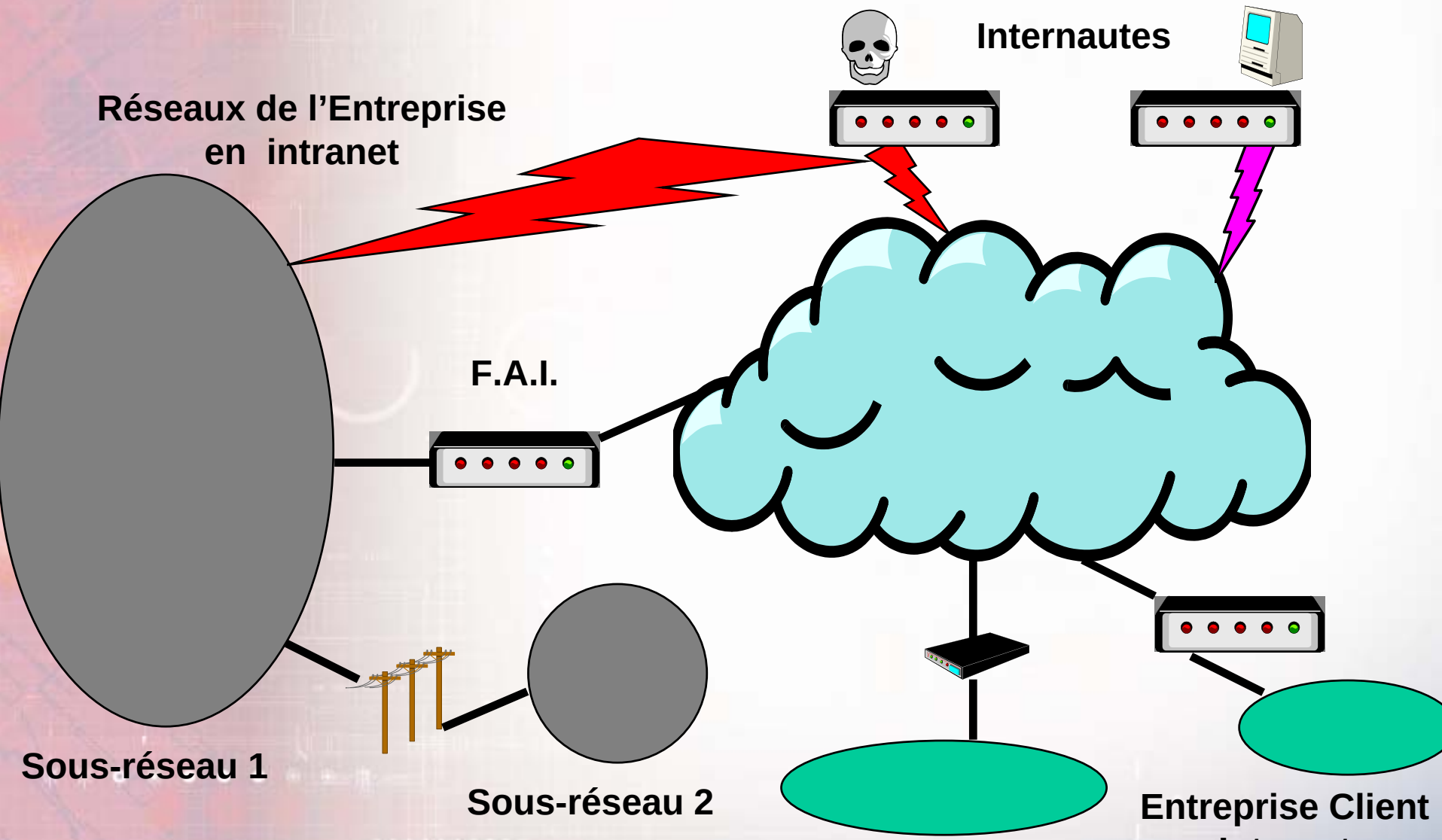
Externalisation (des traitements)

Interconnexion (des réseaux et des entreprises)

Atomisation (réduction de taille des équipements)

Nomadisation (mobilité et connexion à distance)

Interconnexion des réseaux



Vulnérabilités des Systèmes d'Information

Techniques

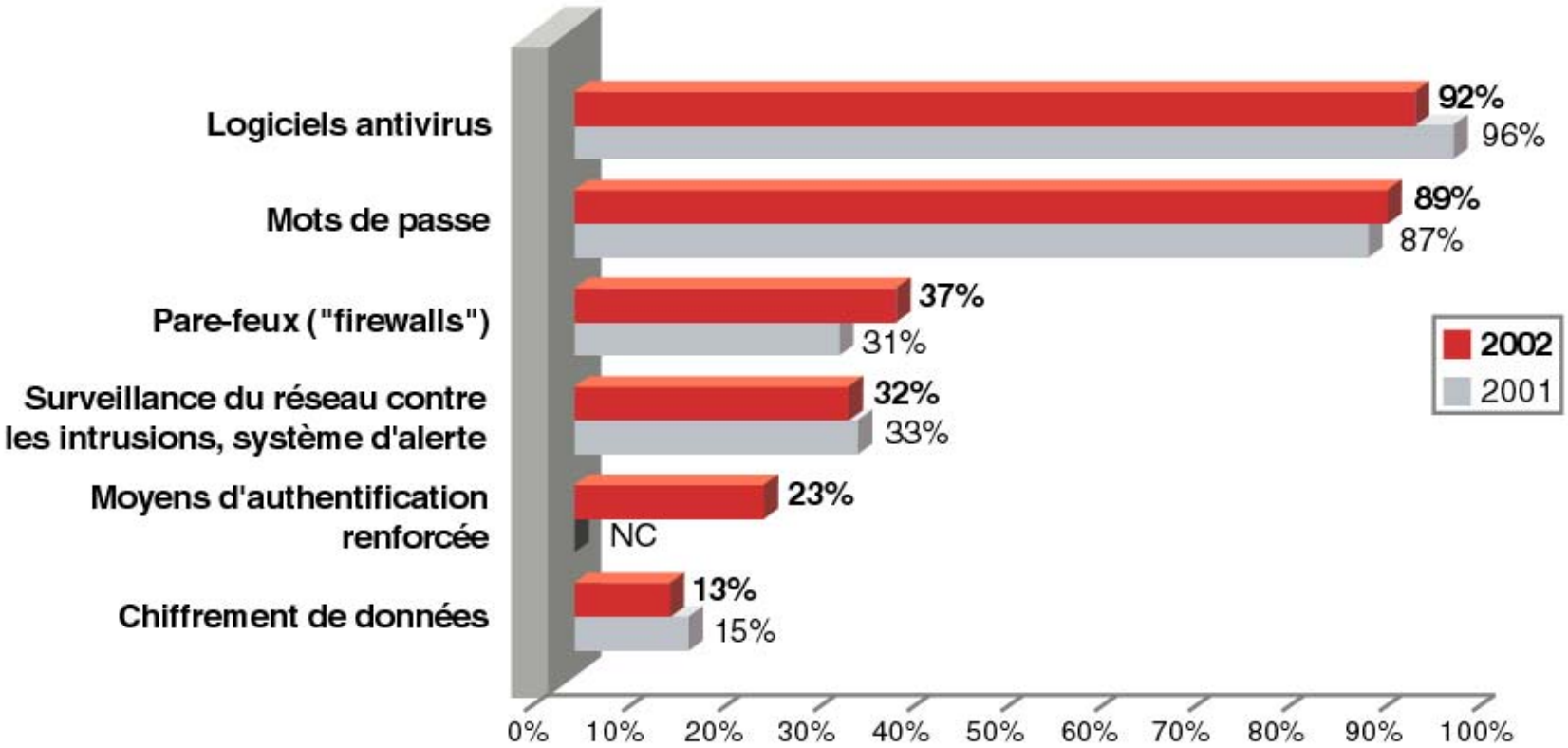
- Faiblesses de conception (architectures, équipements, logiciels, etc.)
- *Bugs* des programmes

Organisationnelles

- Architectures permissives
- Emploi de versions non corrigées des erreurs
- Administration non sécurisée de l'exploitation

Une ouverture croissante des systèmes…

… sans une protection adaptée (source Etude Clusif 2002)



Vulnérabilités des Systèmes d'Information

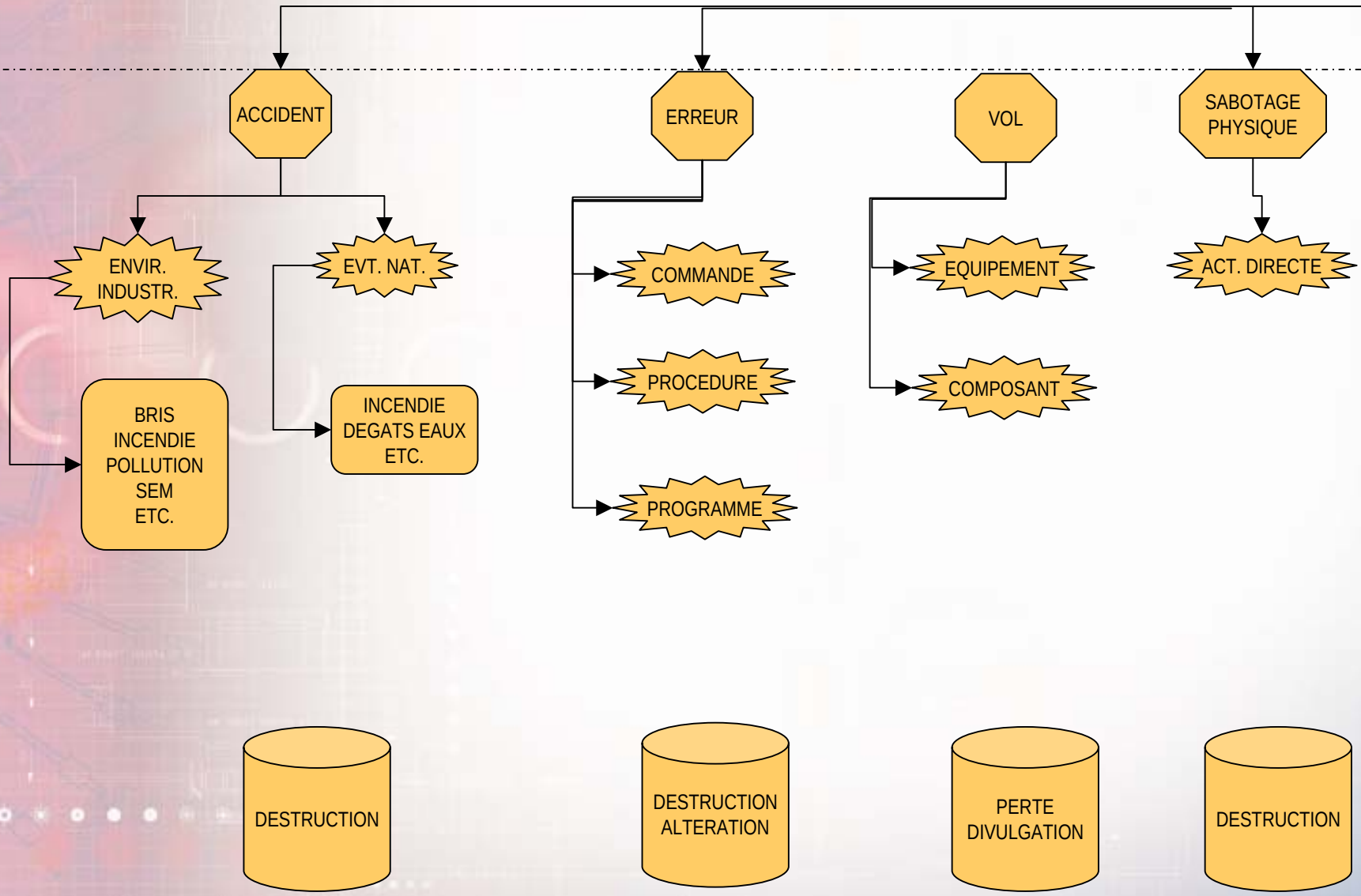
Humaines

- Méconnaissance de la menace
- Insouciance des utilisateurs… et/ou de la Direction
- Internautes : connexions ADSL et/ou câble sans sécurité suffisante (virus, scan IP)

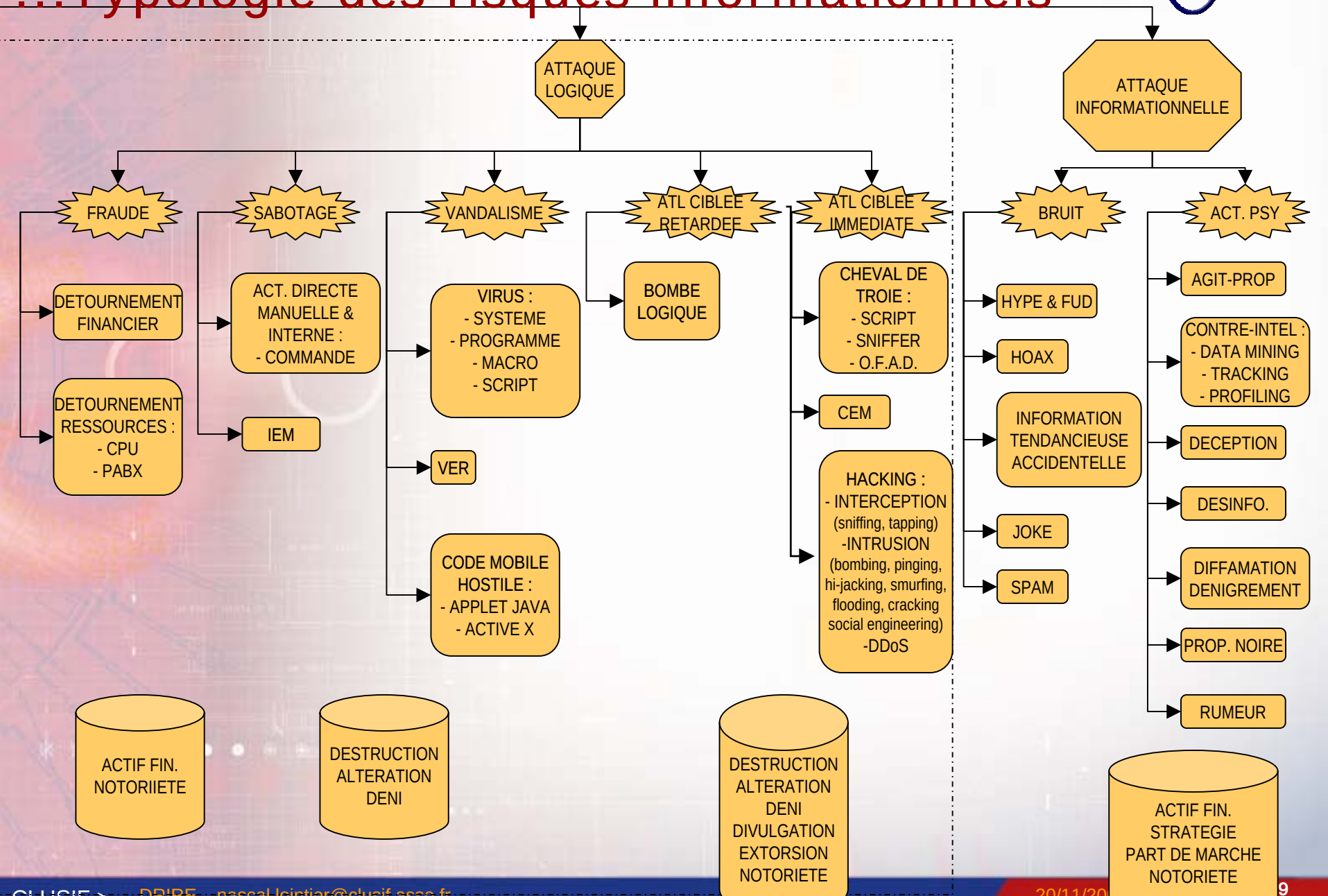
Extérieures : image et notoriété

- Diffamation, dénigrement, décrédibilisation
- Propagandes noires, blanches, grises…

Typologie des risques informationnels



...Typologie des risques informationnels



Menaces sur les systèmes d'information

Un environnement propice

☞ **Une dépendance accrue**

Une diffusion des savoirs pour des acteurs plus nombreux

Une nécessaire dynamique pour la sécurité des systèmes d'information

Le patrimoine informationnel

Les données

- Données de Recherche-Développement
- Données de production
- Données de gestion
- Informations nominatives

Les programmes (propriétaires)

Les ressources (informatiques et télécoms)

- Abus
- Hébergement
- Déni

… Le patrimoine informationnel

La fraude financière

- Les détournements de fonds
- Les extorsions
- La fraude à la vente par correspondance

Le vol de biens

- Informatiques
- Matières premières
- Produits finis

L'image et la notoriété véhiculées *via* les réseaux

La cotation financière

Les années 90 (événements indicatifs)

HTTP et l'Internet grand public

- Réouverture des systèmes
- Diffusion des savoirs

Evolution de la doctrine américaine publique

- Information Warfare (Guerre du Golfe)…
- Information Warriors…
- Information Dominance (*cf.* attaque par l'information)

Passage à l'an 2000, prise de conscience de la fragilité des systèmes d'information (S.I.) et de notre dépendance croissante

Vers une société numérique

Dépendance de l'activité économique

- Informatique de gestion
- Informatique de production et/ou distribution

Dépendance des personnes

- Monétique, téléphonie, organiseurs (PDA)
- Infrastructures partagées

Intérêt d'une action professionnalisée

- Le web est un amplificateur de crise ou d'opportunité :mondialisation et instantanéité
- Déclarations gouvernementales officielles
- Le virus informatique peut contribuer à un enrichisssement

Infoguerre, opportunités…

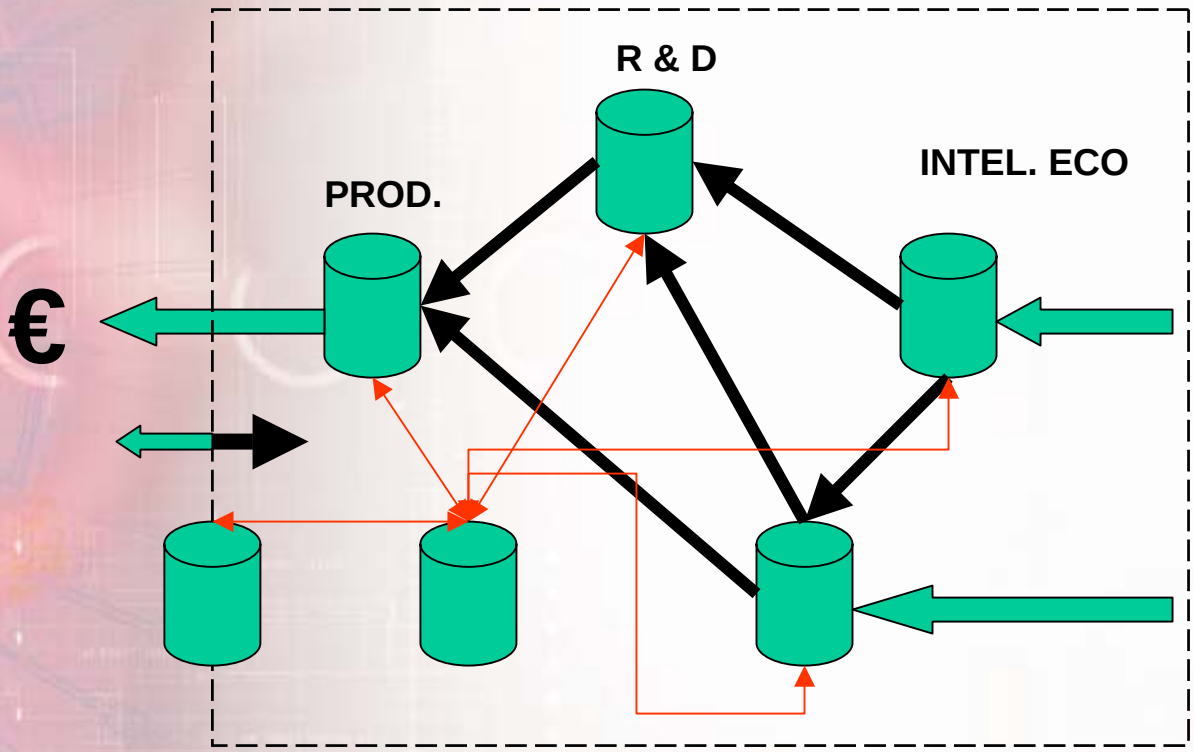
Infoguerre car :

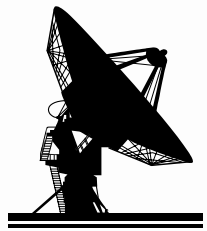
- Situation de compétition ou conflictuelle
- Des éléments de la doctrine militaire peuvent être transposés
- Une information numérique qui en facilite le traitement

Définition élargie :

Méthodes et moyens permettant, par une action sur l'information *numérique*, ***d'altérer les processus de*** *décision*, ***les processus de*** *pilotage* ***et les processus de*** *production* ***adverses avec pour objectifs la*** *désorientation*, *l'attrition* ***et/ou la*** *destruction*.
Trois modes d'action sont possibles : la guerre *contre*, *pour* ***et*** *par* ***l'information, dans un cadre offensif et/ou défensif.***

Les fonctions informationnelles dans l'entreprise (lieux d'impact possibles)





Espace informationnel

- Clients
- Fournisseurs
- Autres acteurs

SEMIOTIQUE :
Interne (culture)
Externe (images produits et entreprise)

RISK MNGT :
(OPSEC & CCI)
Sécurité (R&D, Intel.)
Sûreté (produit)
Qualité (marketing)

MARKETING

Menaces sur les systèmes d'information

Un environnement propice

Une dépendance accrue

☞ **Une diffusion des savoirs pour des acteurs plus nombreux**

Une nécessaire dynamique pour la sécurité des systèmes d'information

Approche sherlockholmesque

Mobile et objectifs

- Motivations humaines classiques
- Utilisation ou destruction de données, ressources informatiques, équipements

Connaissance

- Banalisation et convivialité des outils et procédures d'attaques informatiques
- Diffusion des savoirs
- Réplication de l'information

Opportunité

- Accès distant et/ou « permanent »
- Sentiment d'impunité et/ou d'anonymat

De nouveaux acteurs

Perception du potentiel économique par de nouveaux acteurs

- *Electronic Civil Disobedience Act* de 1997, naissance de l'hacktivisme (culturel, politique…)
- Le grand public, les *wannabes,*
- La concurrence
- La petite délinquance (cf. Yescarding)…

Typologie des acteurs de la malveillance

Personnel de l'entreprise

Personnel de prestataires

Mécontents

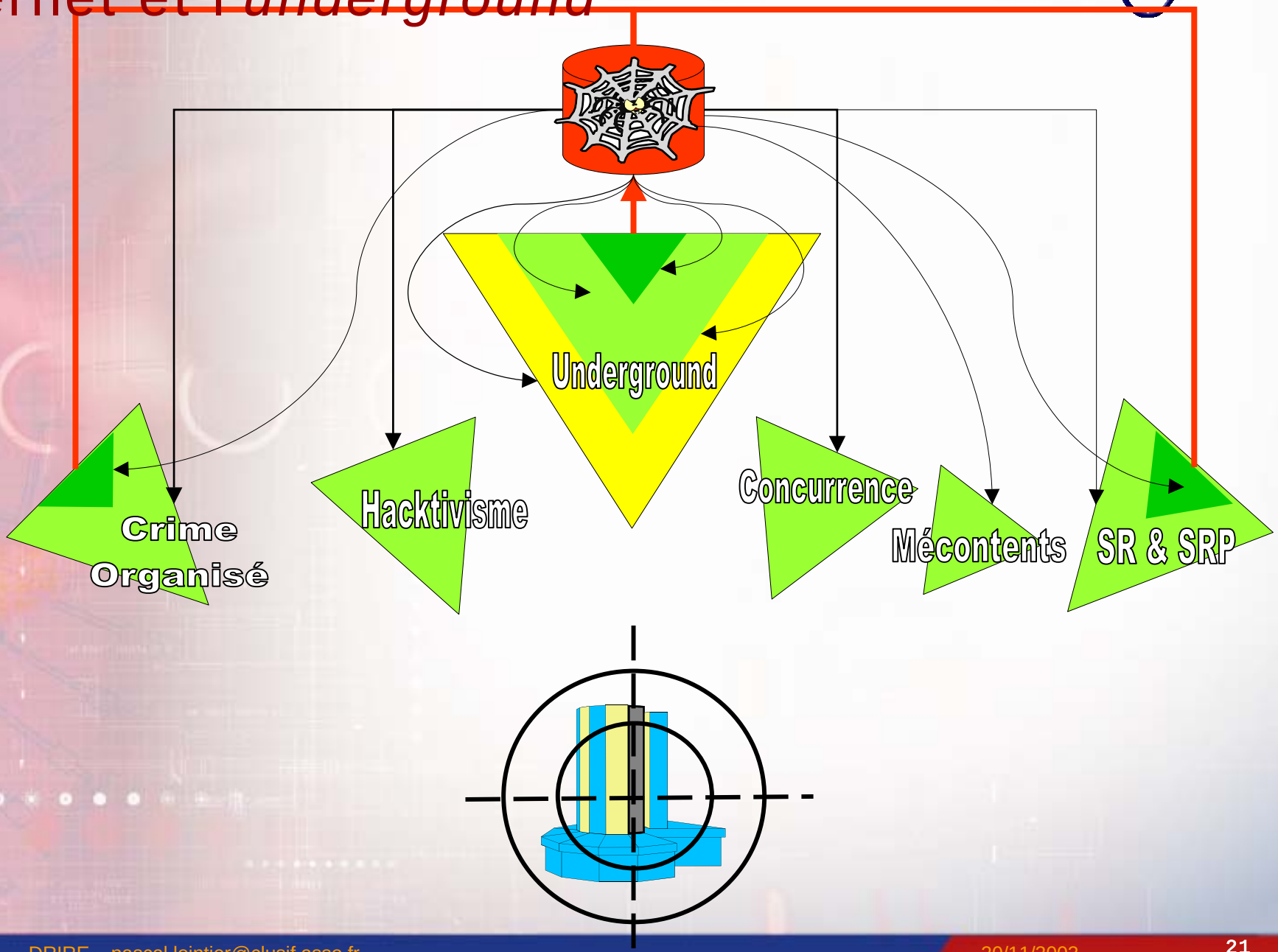
Concurrence

Hackers, *Crackers*, *Phreakers*, etc.

Crime organisé, maffia, petite délinquance

S.R. (service de renseignement) et S.R.P. (société de renseignement privée)

Internet et l'*underground*



Un processus d'attaque répétitif

Renseignement préalable

- **Imposture** téléphonique/électronique (*social engineering*)
- **Fouille des ordures**
- Echange inter-groupes (*rings*)

Intrusion logique

- Identification des machines
- Identification des types de ressources informatiques
- Identification des numéros de version
- Recherche (et, si possible, exécution) de la faille de sécurité relative publiquement accessible. Egalement, *Exploit* 0Day, *Exploit* non publié

Action !

Panorama cyber-criminalité, sommaire 2001

- Yescard et paiements frauduleux
- CodeRed et les virus Internet
- Attaques contre les eBooks et l'œuvre numérique
- La fouille des poubelles, une activité lucrative
- Piratage d'une entreprise ou malveillance interne ?
- Faux sites et parasitisme de nom de domaine
- Rumeurs financières sur Internet
- BadTrans et les atteintes à la confidentialité

La fouille des poubelles

?

- Unilever *vs* Procter & Gamble.
  Objectif : vol de données stratégiques hors systèmes d'information, 3 M$ investis dans l'opération.
- Exploration des poubelles d'une filiale (Sunsilk) d'Unilever à Chicago :
  ➔ 80 documents récupérés par une société d'intelligence économique,
  ➔ plan de lancement des nouveaux produits, politique RH, stratégie commerciale.
  Utilisation d'un stratagème (faux analystes financiers) auprès des cadres d'Unilever.

La fouille des poubelles

Contexte

- Marché des cosmétiques (shampoings) très concurrentiel.
- L'innovation-produit procure de réels avantages compétitifs.
  Résultat : atteinte à l'image, 10 M$ de dommages-intérêts.
- Autres affaires :
  - Oracle vs Microsoft : vol de deux sacs poubelles.
    Objectif : compromettre Microsoft dans les médias pour prouver le financement des groupes de pression
  - Transmeta : tentative de vol des poubelles quelques semaines avant le lancement d'une nouvelle puce

Rumeurs financières et Internet

?

- Escroquerie aux placements financiers sur Internet.
  Un lycéen américain de 17 ans a organisé une escroquerie aux placements financiers
  L'escroquerie lui a rapporté plus d'un million d'euros.
  En un mois et demi (entre le 1er novembre et le 15 décembre 2001), le jeune homme avait créé une société d'investissements ("Invest Better 2001") avec pour vitrine, un site Web et un bulletin Internet.
  Appât : proposition de placements « garantis et sans risques » avec promesses de rendement de 125 % à 2500 %.
  Plus de 1000 victimes se sont fait escroquer.
  Il est épinglé par la SEC (Securities and Exchange Commission)

Rumeurs financières et Internet

Contexte

- Les escroqueries financières sur Internet sont significatives et se déclinent en différentes formes
  - Rumeurs pour faire monter ou chuter des cours de Bourse.
  - Conseils payants pour placements boursiers fantômes.
  - Conseils pseudos indépendants.
  - Systèmes pyramidaux (affaire William Caudell).
  - Sites Web vitrines de fausses sociétés.
  - Sites Web au design usurpant celui de vraies institutions financières (cf. affaire émission de fausses garanties bancaires, 29 sites Web avec l'apparence de Bloomberg).
  - Achats en ligne sans livraison des biens.
  - Etc.

Panorama cyber-criminalité, sommaire 2002

Vote électronique

Données personnelles-vol d'identité-fraude

Chantage-Extorsion

Mass Mailing accepté

P2P

Attaques DoS contre serveurs de noms

Dangers des réseaux sans fil

Yescard 2G

Chantage-Extorsion ?

- Août 2002 – JAPON. L'entreprise japonaise Fujitsu reconnaît avoir été victime d'un chantage. Infos confidentielles liées à système informatique de la Défense obtenues par un programmeur sous-traitant pour Fujitsu.
  Preuve apportée par maître-chanteur dans document imprimé de 10 pages : infos sur la manière dont sont reliés les ordinateurs de la Ground Self Defence Force plus d'autres infos sur Système de Défense aérienne, infos sur réseau entre ordinateurs y compris les adresses IP des ordinateurs.
  Pression : revente des données envisagées à Corée du Nord.
  Refus de Fujitsu de céder au chantage. Porte plainte à la police pour tentative d'extorsion de fonds

Chantage-Extorsion

- Fujitsu écarté des contrats de Défense. Motif : n'a pas donné le nom de ses sous-traitants participant à la mise en place du système informatique.
- Programmeur et un complice inculpés en novembre 2002. Autres complices relâchés pour insuffisance de preuves

Chantage-Extorsion

?

- Octobre 2002. Roumanie-USA. En Roumanie, un jeune homme condamné à 3 ans de prison (Nicolae Mircea Harapu) pour intrusion dans le système informatique d'une entreprise américaine (Zwirl.com).
  Vol d'information sur clients, dont numéros cartes bancaires.
  Chantage : 5 000 dollars demandés pour ne pas les divulguer, indique à la société Zwirl que les crimes sur Internet ne sont pas punis par la loi en Roumanie, indique une banque où se faire virer un accompte de 500 dollars. Envoie un ami les retirer. Se fait arrêter lors d'une opération conjointe FBI-police roumaine

Chantage-Extorsion

?

- Mai 2002. Affaire Bloomberg, Kazhakstan-USA-GB. Oleg Zevov et Igor Yarimaka sont extradés aux USA, inculpés de piratage, tentative d'extorsion et menaces. Ils ont pénétré le système informatique de Bloomberg en 2000. Zevov a contacté par e-mail le patron de Bloomberg, Michael Bloomberg, pour lui demander 200.000 dollars en échange de la méthode d'intrusion. Il les a déposés sur un compte. Zvevov était employé de la société Kazcommerts au Kazakhstan. Cette société avait un contrat avec Bloomberg, « Open Bloomberg », service de bases de données. Michael Bloomberg ouvre un compte bancaire à Londres, il y dépose les 200.000 dollars. Les deux pirates se rendent à Londres au rendez-vous fixé avec Bloomberg

Les TIC au service des crimes et délits

Il est normal d'utiliser une ressource (performante)

- Donc, pas de catastrophisme vis-à-vis de l'emploi d'Internet (FIS, GIA, El Qaeda, etc.). Par ex., la stéganographie a été utilisée *de tout temps*

Toute nouvelle ressource peut (va) générer un emploi malveillant

- Détournement d'usage, effet de bord, etc.

Toute nouvelle ressource porte un risque intrinsèque. Par ex., messagerie électronique

- Perte de hiérarchie
- Risque de *bombing* (saturation ou déni de service)
- Divulgation accidentelle (CC et *reply-to*, affaire M. Lewinsky)

Menaces sur les systèmes d'information

Un environnement propice

Une dépendance accrue

Une diffusion des savoirs pour des acteurs plus nombreux

☞ Une nécessaire dynamique pour la sécurité des systèmes d'information

Des solutions existent

Gravité $_{risque}$ = F°[Impact f°(Sol. Sec.), Potentialité f°(faisabilité, récurrence)]

Moyens de prévention/protection

- Réduction de probabilité de réalisation
- Réduction d'impact
- Transfert du risque résiduel vers l'assurance

Réactions sur incident

- Mesures techniques et organisationnelles
- Action judiciaire (si malveillance)
- Communication (web de crise)

Lutter contre l'insouciance et la méconnaissance dans l'entreprise

Qualifier les informations sur la malveillance

Ne pas penser une sécurité « forteresse » mais une défense en profondeur

Nécessité d'une dynamique sécuritaire

Réagir aux situations atypiques

Dissuader – Ralentir – Alarmer (puis agir !)

LES SYNTHÈSES DU CLUSIF

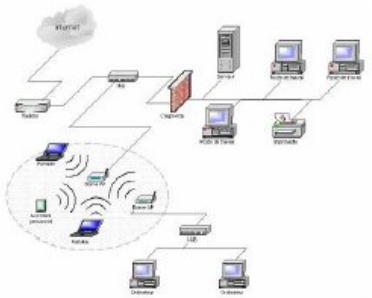
Réseaux sans fil : menaces, enjeux et parades

1. Introduction

Le présent document a un double objectif : d'une part sensibiliser les entreprises et les administrations aux risques inhérents au déploiement d'un réseau sans fil (RSF) de type 802.11b et d'autre part, présenter les solutions qui permettent d'augmenter la sécurité pour ce mode de connexion. Ce document ne traite pas des autres normes, telles que : 802.11a, 802.11i, 802.1x, Hiperlan, etc. ni des infrastructures personnelles ou des *hot spots*.

2. Infrastructure

Le RSF de type 802.11b repose sur une norme (cf. annexes). Il s'agit d'un protocole de transmission radio de proximité sur des canaux préétablis.



Une infrastructure typique qui combine ad hoc et connexion Internet

LES SYNTHESES DU CLUSIF — Document revu le 08/03/2003 — 1/5

© CLUSIF 2003 – Droits de reproduction : cf. page 5

www.clusif.asso.fr

Étude et statistiques sur la sinistralité informatique en France

Année 2002

cybercriminalité, année 2002

Présentation de quelques malveillances

es Systèmes d'Information Français