Sécurité des systèmes d'information

Analyse des risques

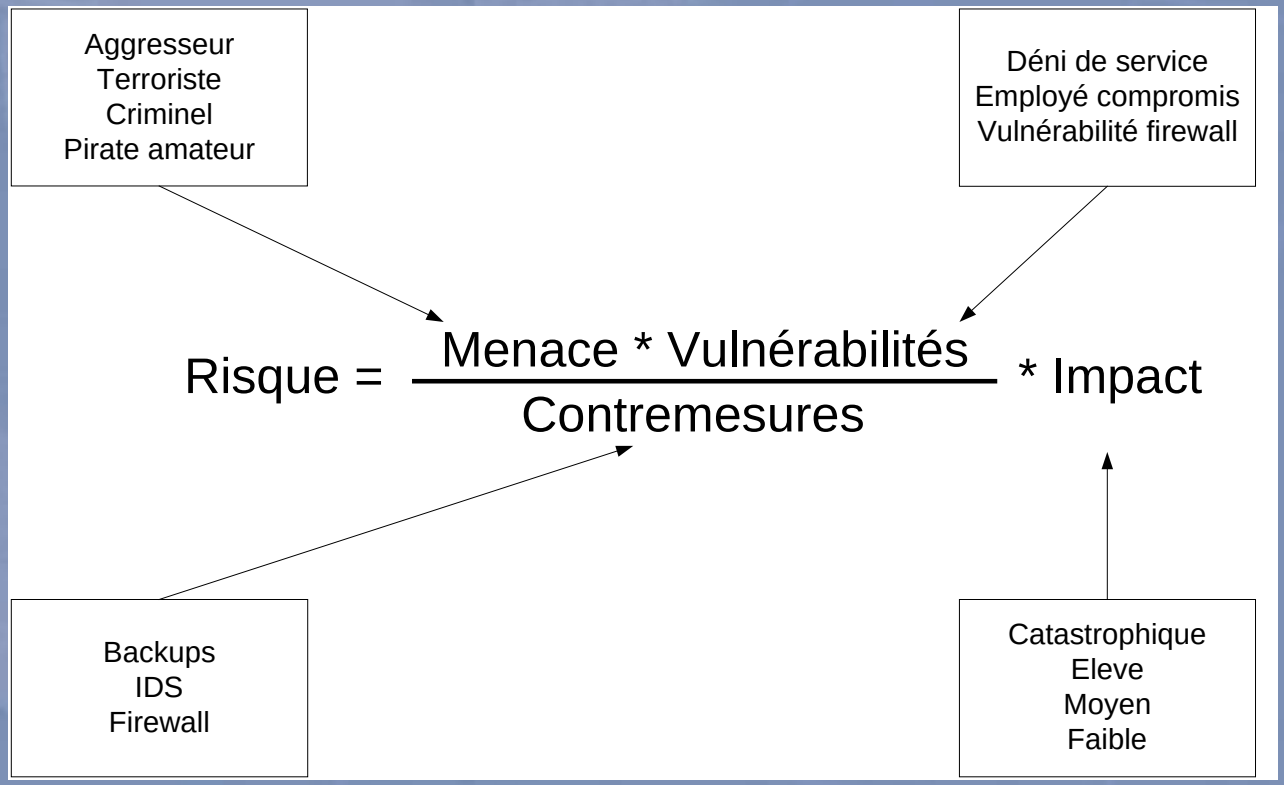
Nécessité d'une AR

- Identifier les risques sur un SI
- Les classer
- Les chiffrer
- Pour concevoir les parades

Modèles d'analyse

- Des modèles analytiques sont disponibles pour chiffrer les risques en général
- Nous allons en voir quelques exemples, appliqués au cas de réseaux connectés à Internet

Equation des risques (1)



(SANS, janv. 2001)

Equation des risques (2)

- Dans ce modèle:
  - Les vulnérabilités augmentent le potentiel de la menace
  - Les contremesures réduisent ce potentiel
  - L'impact augmente le problème entier

Equation des risques (3)

- Evaluation probabilistique :

  Risque = P_a x (1 – P_i) x C

  – Pa: probabilité de l'attaque

  – Pi: Efficacité des contremesures

  – C : conséquences de la perte de la ressource considérée

La menace (1)

- Mes systèmes sont-ils une cible potentielle ? Et pour qui ?
- La menace la plus évidente: les personnes
  - Des pirates incompétents aux pirates talentueux
  - Des curieux aux très motivés

La menace (2)

- Les personnes peuvent être regroupées en 2 catégories:
  - Les « insiders »: personnes perpétrant l'agression de l'intérieur (ex: employés, contractants, ...) physiquement ou logiquement
  - Les « outsiders »: personnes agissant de l'extérieur, et devant avant tout se doter d'une porte d'entrée

La menace (3)

- Jusqu'à récemment, la menace supposée la plus importante est celle des « insiders »
- Maintenant, on tend à équilibrer les deux
- Certains donnent même les extérieurs comme la plus grosse menace (SANS, Janv. 2001)

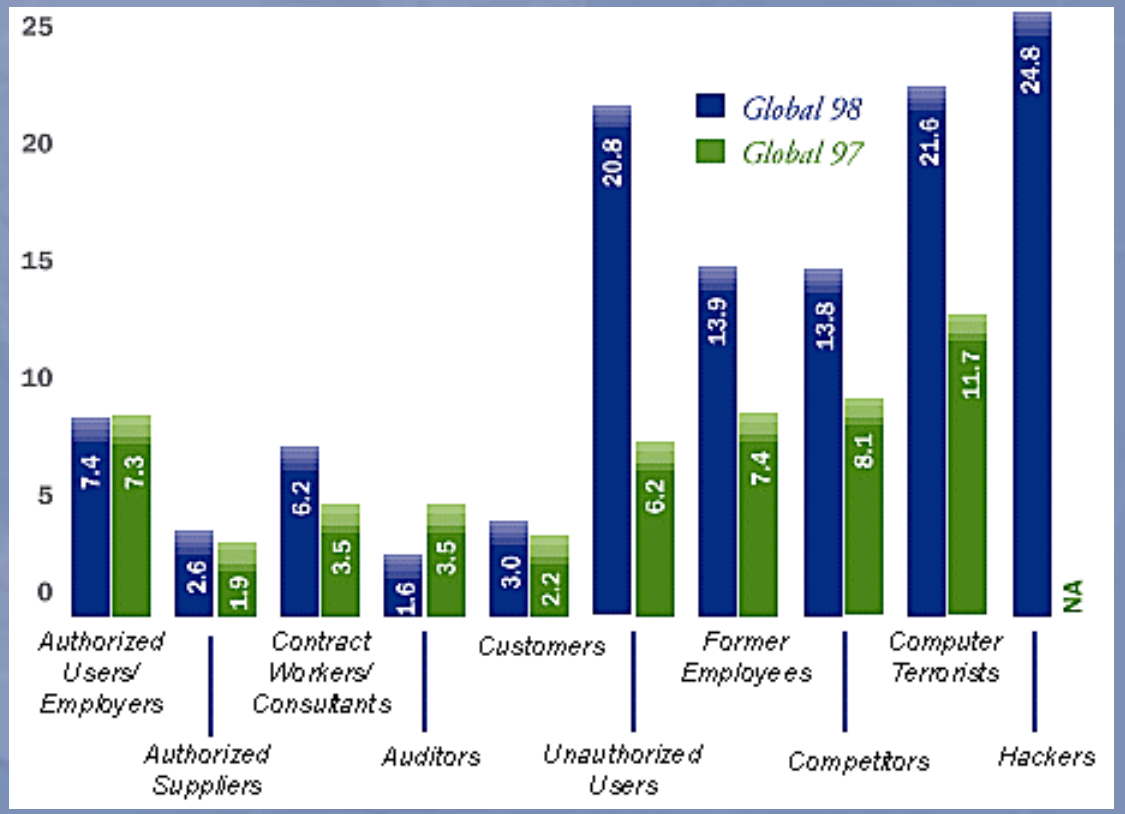
La menace (4)

- Quels sont leurs motifs ?
  - Curiosité
  - Défi
  - Espionnage industriel
  - Vandalisme
  - Escroquerie
  - Chantage
  - ...

La menace (5)

	Existence confirmée	Existence probable mais non confirmée	Existence probable en 2005
Incompétents	Nombreux		
Pirates réguliers	Nombreux		
Employés	Nombreux		
Escrocs	Nombreux		
Crime organisé	Peu nombreux		Nombreux
Dissidents politiques		Nombreux	
Groupes terroristes		Peu nombreux	Nombreux
Espionnage d'état	Peu nombreux		Nombreux

La menace (6)



Source: Ernst & Young

La menace (7)

- Les compétences des agresseurs (SANS Janv. 2001)
  - 30% curieux ou par accident
  - 50% vandales ou pirates amateurs avec quelques compétences réseaux
  - 16% professionnels de l'informatique, experts sécurité et programmeurs
  - 4% vrais créateurs et innovateurs

Les vulnérabilités (1)

- Le concept de vulnérabilité s'applique essentiellement aux systèmes supposés sûrs
- Peut aussi être absence délibérée ou non de protection

Les vulnérabilités (2)

- Vulnérabilités = fautes opérationnelles connues ou non dans un système de protection
- Et pouvant engendrer un incident de sécurité
  - On parle de faille « exploitable » ou « non exploitable »

Les vulnérabilités (3)

- Principalement
  - Des fautes de conception (algorithme)
  - Des fautes d'implémentation (coding mistake)
  - Ces fautes étant délibérées ou non
- Dès qu'elles sont publiques, font très rapidement l'objet de correctifs (*patches*) à installer

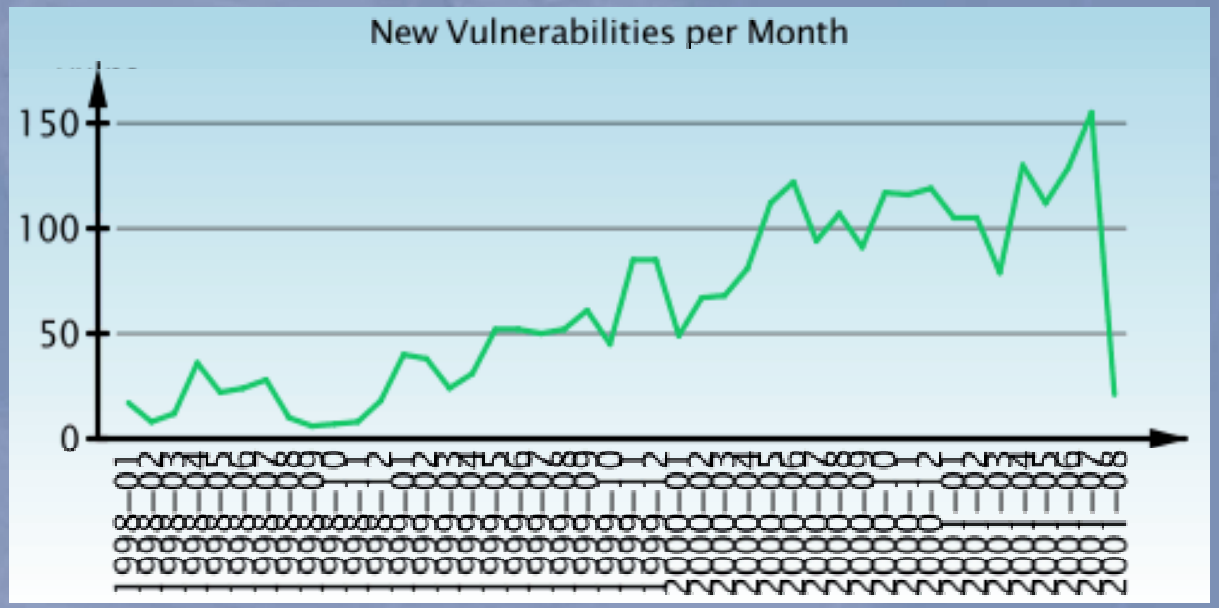
Les vulnérabilités (4)

- De grandes classes de vulnérabilités sont connues
- De nouvelles vulnérabilités sont découvertes quotidiennement
- Les patches sont annoncés dans les forums, sites Web, listes de diffusion
  - Sites web des constructeurs
  - www.securityfocus.com
  - Mailing list Bugtraq (cf. securityfocus)

Les vulnérabilités (5)

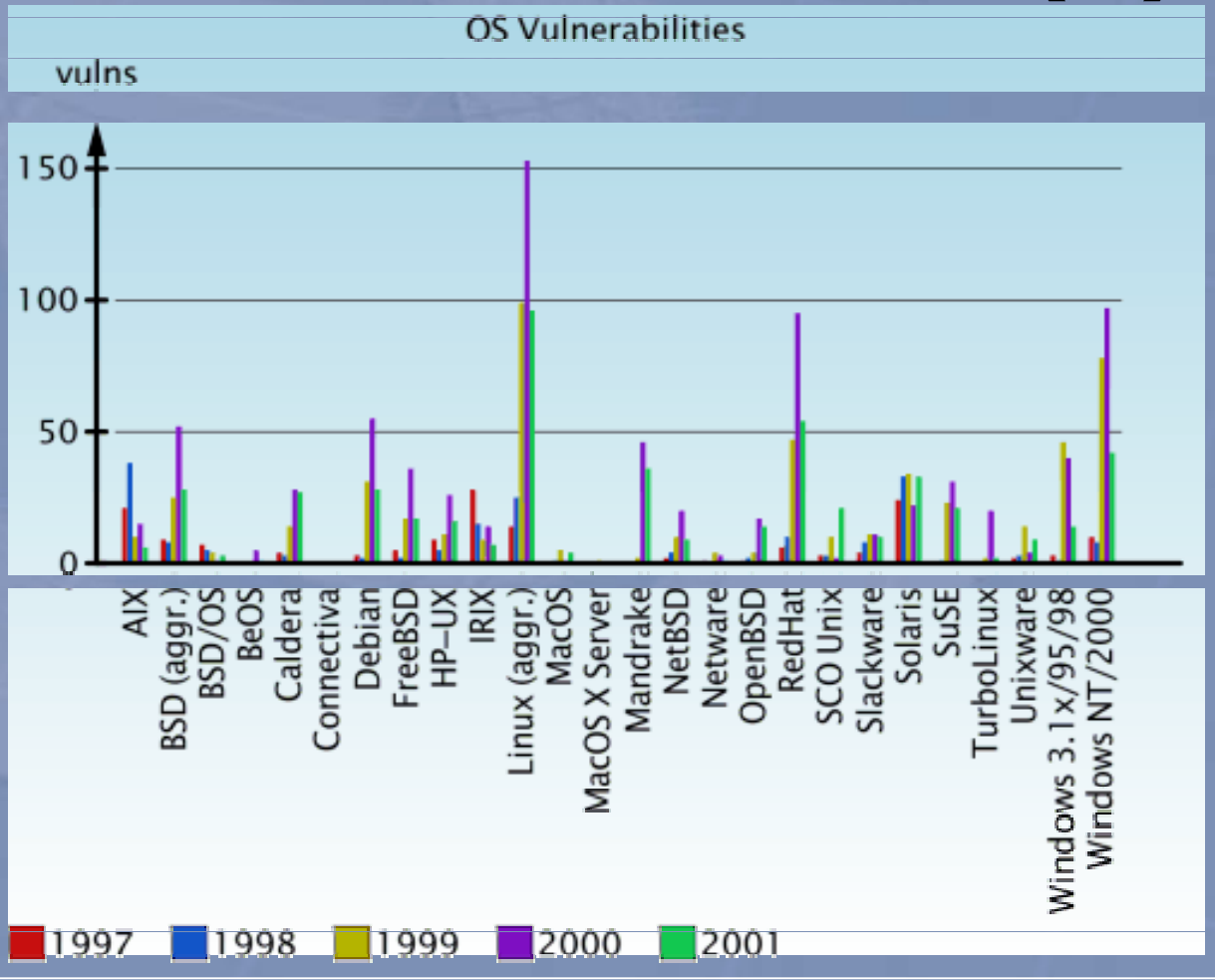
- Janvier 2001: 3747 vulnérabilités répertoriées par le CERT depuis 1995
- Statistiques (NIST, 2000):
  - 40% sont locales (lancées depuis la machine), 60% sont distantes
  - 23% affectent l'OS, 24% les parties réseaux de l'OS, 53% les applications, 5% le hardware, 0.4% les moyens de crypto
  - 53% violent les privilèges (élévation de privilèges), 20% la confidentialité, 19% l'intégrité

Les vulnérabilités (6)



Source: Securityfocus.com

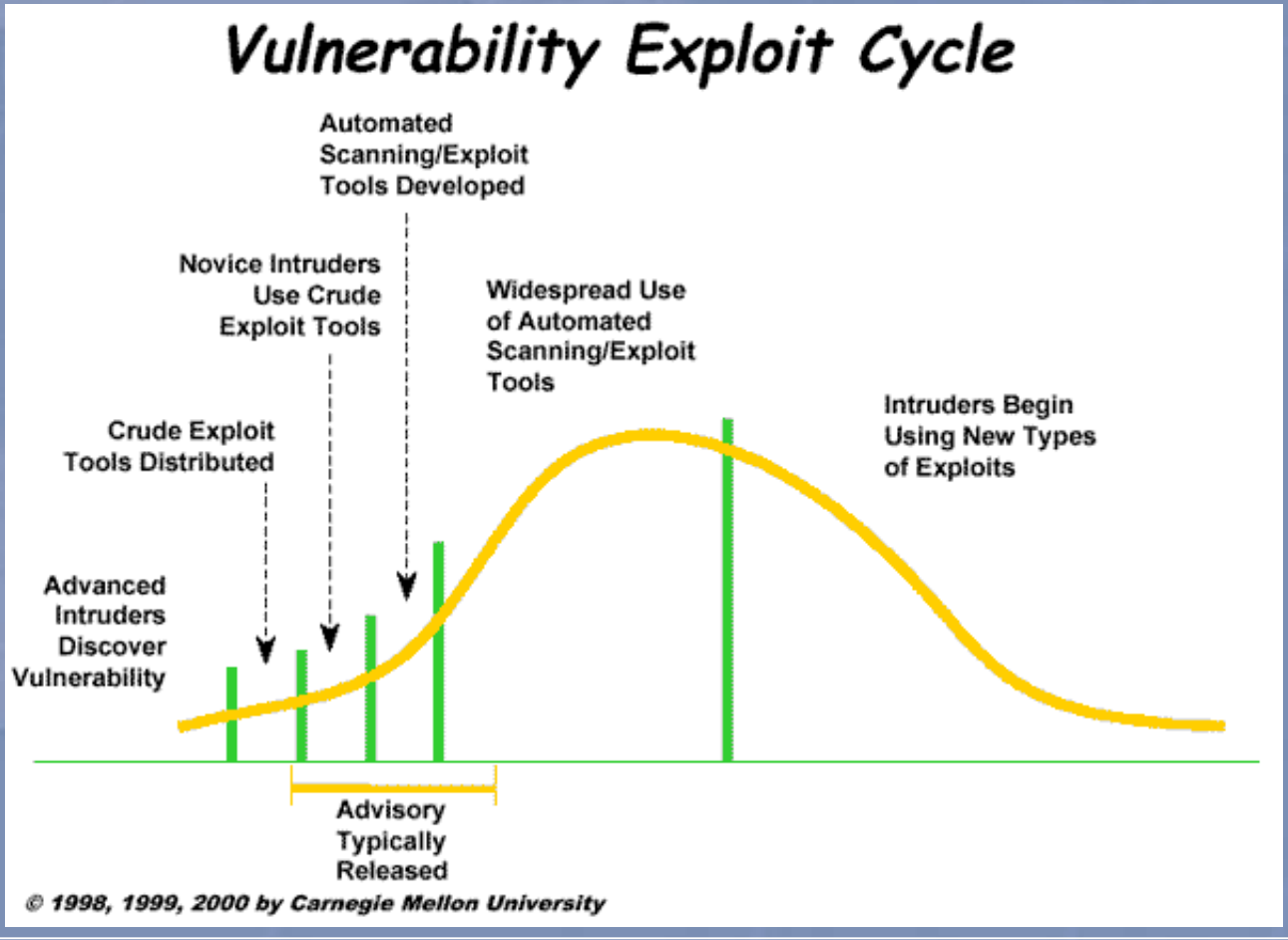
Les vulnérabilités (7)



Les vulnérabilités (8)

- Certaines vulnérabilités sont délicates à exploiter
  - Donc limitées aux agresseurs experts
- Cependant, avec le temps des outils automatiques apparaissent
  - Ils facilitent l'exploitation de la vulnérabilité
  - Ex: ADM NXT How-To: http://library.psyon.org/hacking/honeynet/forensics/NXT-Howto.txt

Les vulnérabilités (9)



Les vulnérabilités (10)

- Le cycle de vie des vulnérabilités, un facteur important
- Explique pourquoi il est extrêmement difficile de contrer un agresseur compétent et déterminé

Les contremesures (1)

- Les matériels et logiciels de sécurité
  - Fonctionnalités natives des OS
  - Logiciels dédiés: Firewalls, IDS
- La compétence des admins sécurité
- La formation des utilisateurs
- Les lois en vigueur
- Les avertissements
- ...

Les contremesures (2)

- Les contremesures feront l'objet d'un chapitre dédié
- Elles ont la propriété de s'additionner:
  - Encryption + mots de passe forts + syslog + administrateur compétent + ...
- Mais peuvent elles-même introduire des risques !!!

L’impact (1)

- D’après l’équation des risques, l’impact est directement multiplicatif par rapport à la menace
- L’impact est très important à déterminer
- Il permettra de concevoir des contremesures adaptées
  - Adaptées = dont le coût est en rapport avec la valeur de la ressource

L’impact (2)

- L’impact est une combinaison de:
  - La valeur de la ressource pour l’entreprise
  - D’une estimation des moyens à mettre en œuvre pour corriger d’éventuels problèmes

L'impact (3)

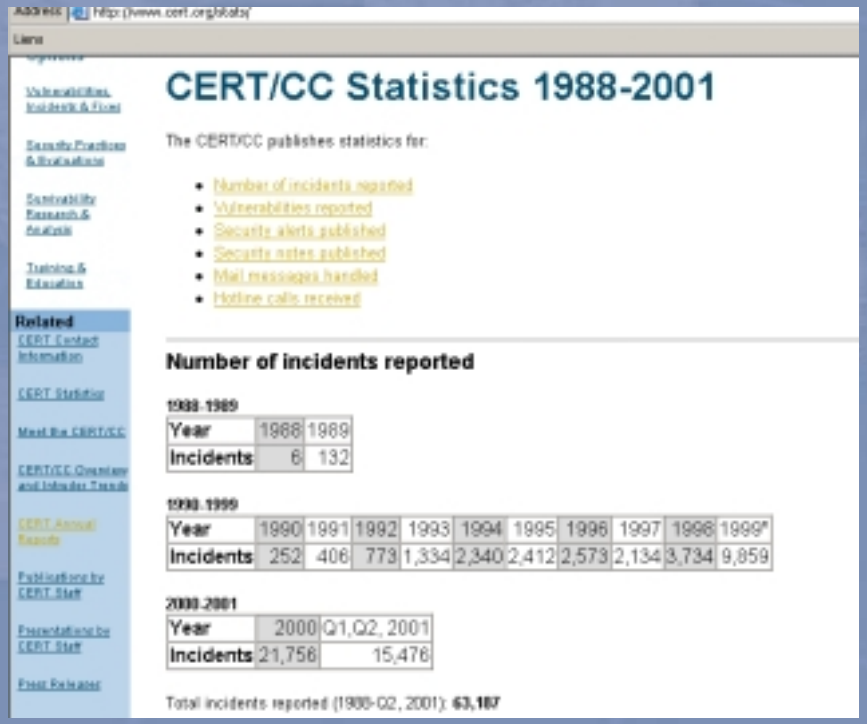
- La valeur d'une ressource n'est pas évidente à déterminer
  - Un site Web isolé du reste du réseau peut être compromis sans danger pour les données sensibles
  - Par contre la dégradation de l'image de marque peut engendrer des coûts importants
  - L'implication involontaire dans un piratage (rebond) peut entraîner de fâcheuses suites judiciaires.

Le résultat: quantification du risque

- Critères appréciation internes à l'organisation
- Résultats relatifs entre eux
- Utile pour évaluer la probabilité d'un type d'incident donné

Intrusions reportées

- Nombre d'intrusions déclarées



CERT/CC Statistics 1988-2001

The CERT/CC publishes statistics for:

- Number of incidents reported
- Vulnerabilities reported
- Security alerts published
- Security notes published
- Mail messages handled
- Hotline calls received

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

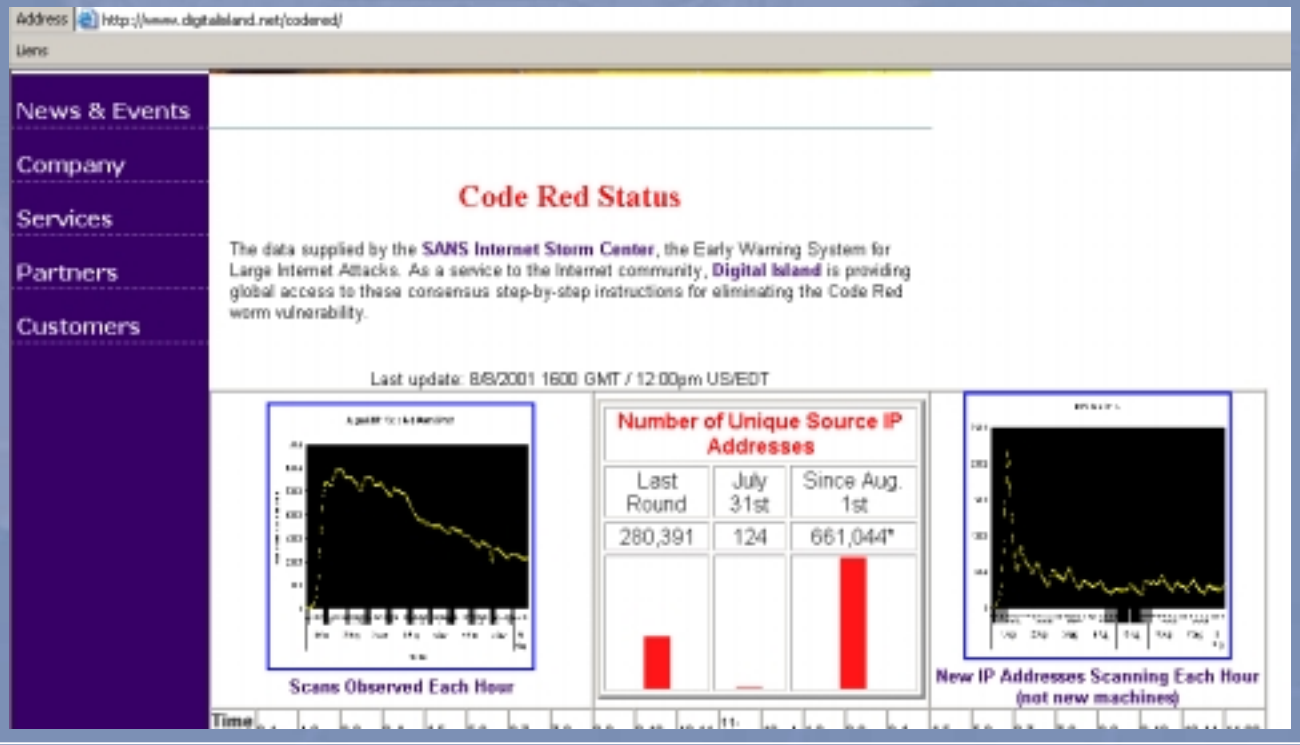
2000-2001

Year	2000	Q1,Q2, 2001
Incidents	21,756	15,476

Total incidents reported (1988-Q2, 2001): **63,187**

Evènements remarquables

- CodeRed Worm



Conclusion

- Identifier les risques, menaces, une nécessité avant d'envisager toute contremesure
- Réitérer le calcul de risque après l'installation de ces contremesures
- Le calcul de risque ne s'applique pas qu'à Internet
  - Toute menace possible sur le SI est à prendre en compte (intrusion physique, téléphonique, ...)

Exercice (1)

- Quantifier le risque de:
  - La présence d'une faille sur les serveurs Web Microsoft IIS permettant de lire tout fichier sur le serveur
  - La perte complète de l'accès Internet après un déni de service

Exercice (2)

- Pour les entités suivantes:
  - Une entreprise A fournissant des composants électroniques, et disposant d'un site Web hébergé chez un prestataire. Ce site Web contient en accès restreint aux clients (identifiés par mots de passe), le catalogue de la société.
  - Une entreprise B de gestion de fonds de pension, ayant un serveur Web contenant quelques pages statiques, et utilisant Internet pour la consultation des informations financières ainsi que les passages d'ordres.

Exercice (3)

- Identifier le plus grand nombre de risques liés à la liaison Internet pour un fabricant de produits de luxe.
- Identifier le plus grand nombre de risques liés à Internet pour une société d'armement. Les données confidentielles sont supposées situées sur un réseau complètement séparé.