

HERVE SCHAUER

HSC

Les risques

Les risques ne cessent d'augmenter:

- **Informatisation systématique de l'ensemble de la société**
- **Ouverture des systèmes d'information sur Internet**
- **Démultiplication de ce qui est branché sur Internet**
- **Uniformisation de la société de l'information**

Conséquences générales sur la société

Exemples de risques

- Dénis de service et dénis de service répartis
 - Défiguration de serveur web
 - Vols des fichiers de cartes bancaire
 - Dossiers médicaux publiés sur internet
 - Plantage d'un tiers certificateur
 - Vol d'un accès à une banque en ligne sur un poste client
 - Contrefaçon aux droits d'auteurs
- ...

Les vulnérabilités sont diversifiées et sont principalement applicatives

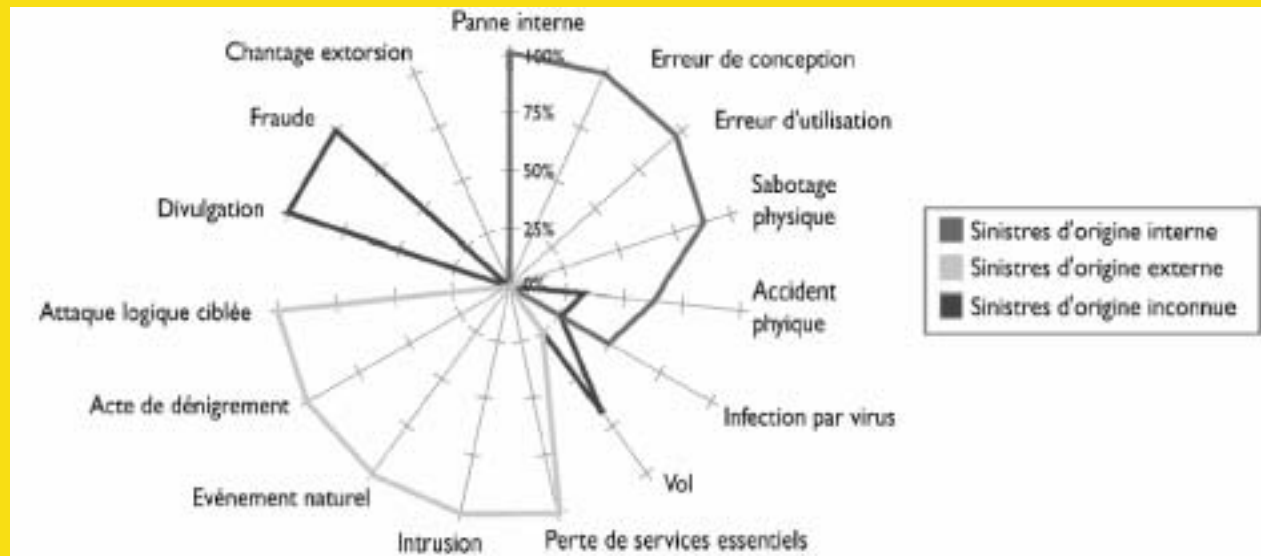
Conséquences

- Pertes de temps
 - Pertes financières
 - Mauvaise image de marque
 - Dévalorisation boursière
 - Problèmes judiciaires
 - Pertes de savoir-faire
- ...

Les conséquences d'une atteinte à la sécurité portent bien au delà des aspects techniques

L'étude du Clusif

Origine des incidents par nature :



Copyright Étude sinistralité Clusif 2001

Les sinistres venus de l'extérieur demeurent importants.

Les failles techniques

SANS Top 10 Unix

- U1 Exécution de procédure distance (RPC)
- U2 Serveur web Apache
- U3 Secure Shell (SSH)
- U4 Simple Network Management Protocol (SNMP)
- U5 File Transfer Protocol (FTP)
- U6 R-commandes
- U7 Impression distante (LPD)
- U8 Messagerie Sendmail
- U9 Serveur de noms Bind
- U10 Authentification Unix en général : comptes sans mot de passe ou avec des mots de passes faibles

Les failles techniques

SANS Top 10 Windows

W1 Serveur web Internet Information Services (IIS)

- Incapacité à gérer les requêtes imprévues
- Débordements de tampons
- Applications de démonstration

W2 Microsoft Data Access Components (MDAC) -- Remote Data Services

W3 Microsoft SQL Server

W4 NETBIOS : Partages Windows par le réseau sans contrôle d'accès

W5 Connexion anonyme (Anonymous Logon)

W6 Authentification LAN Manager : faiblesse du hachage Hashing

W7 Authentification Windows en général : comptes sans mot de passe ou avec des mots de passe faibles

W8 Internet Explorer

W9 Accès distant à la base de registre

W10 Windows Scripting Host

Expérience HSC

Les serveurs WWW sont la principale cible

- Mauvaise gestion des sessions
- Cookie codé contenant le nom de l'utilisateur authentifié
- Injection SQL permettant de consulter et modifier la base, parfois avec des privilèges
- Débordement de tampon dans les scripts
- Mots de passe utilisateurs beaucoup trop simples sur Internet permettant d'accéder à des serveurs de courrielweb

Les problèmes réseau la seconde

- Réseaux sans fil non protégés

Les systèmes d'exploitation la troisième

Les menaces externes se développent car du personnel de l'intérieur attaque de l'extérieur

La menace du firewall

Le firewall a du succès car il a été et demeure une brique de base indispensable

- Permet un contrôle d'accès sur le périmètre de l'entreprise
- Protège d'emblée l'ensemble du réseau privé
- Permet un audit relativement simple pour les auditeurs

Le firewall n'est plus suffisant

- Le périmètre du réseau privé est flou et poreux
- Le firewall est détourné
 - Ré-encapsulations
 - Accès distants
 - B2B
 - Réseaux sans fil

Le cadre réglementaire

Protection des données à caractère nominatif

Protection des logiciels

Protection contre l'intrusion dans un système informatique

Reconnaissance de la signature électronique

Moyens d'applications et jurisprudence limités

Pas de bonnes pratiques réglementaires

La sécurité dans le temps

Chaque changement dans l'internet tend à moins de sécurité

- EDI ou B2B
- Voix sur IP
- Réseaux sans fil

Les produits de sécurité suivent une évolution difficile

- Analyse de contenu
- Filtrage TCP/IP par les firewalls -> Contrôles applicatifs dans HTTP
- Protocoles TCP sur IP -> SOAP/XML sur HTTP

De plus en plus d'utilisateurs pour de plus en plus d'usages

De moins en moins de sécurité

Le problème humain

**La sécurité n'est pas une issue technologique mais humaine
il ne faut pas se concentrer sur la sécurité mais sur son métier**

- les motivations du métier
- les coûts du métier
- la vision du métier

Sécurité => Consensus

Concilier :

- Les responsables du métier
- Les responsables de l'informatique
- Les responsables de l'entreprise
du contenu la politique de sécurité
et de son application avec des experts

La sécurité doit donner un sens au métier de l'entreprise et à ses affaires

Analyse de risques

Menace

Ce dont l'entreprise souhaite se protéger

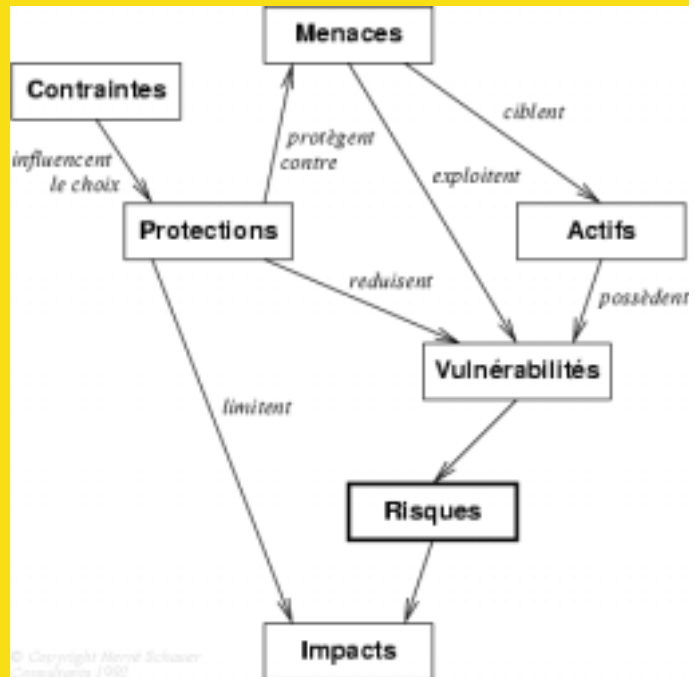
Vulnérabilité

Faible ou faiblesse du système d'information

Risque

Quand une menace a exploité une vulnérabilité sur un actif

Risque = Coût x Menaces x Vulnérabilités



Gestion de risques

Une vision de la gestion de risques :

Le coût d'amélioration de la sécurité

- dépense significative
- réduit la fonctionnalité
- gêne les utilisateurs
- gêne les clients

Le coût d'ignorer la sécurité

- parfois mauvaise presse
- des clients mécontents
- dans certains cas une pression législative

=> beaucoup en font le minimum et pas plus que le voisin

Étape 1 : Formaliser les responsabilités

Sans responsabilisation

- Pas de conséquences réelles d'une mauvaise sécurité
- Pas de possibilité d'assurance

Responsabiliser les gens

- Formaliser leur travail
- Formaliser les règles de sécurité
- Formaliser qui contrôle

Étape 2 : Choisir une stratégie

Ignorer le risque

Réduire le risque

Transférer le risque

- Accepter le transfert de responsabilité
- Assurance peut convertir en partie une responsabilité à géométrie variable en une responsabilité mesurable pour les responsables

Cela permet de savoir gérer l'infogérance

Étape 3 : Choisir des solutions

Inclure la sécurité dans tous les projets dès le départ

Déployer des protections pour réduire les risques

Adapter les solutions de sécurité à ses métiers

Utiliser des check-lists

Fournir des tableaux de bord aux dirigeants

Conclusion

- **Les risques sont là, seront toujours là et augmentent**
- **Les produits de sécurité sont un composant de la solution**
Ce sont des outils indispensables mais pas suffisants
- **Le mieux à faire est de gérer les risques avec bon sens, cohérence et équilibre**
- **La société qui gère le mieux les risques sera la plus bénéficiaire**
- **La sécurité est souvent une réflexion après coup**
En intégrant la responsabilité et l'assurance dès le départ des projets la sécurité peut devenir créatrice de productivité.