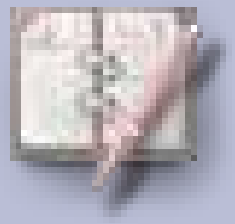
# La sécurité des portails d'entreprise

Cédric BLANCHER
Arche, groupe Omnetica / MISC
cedric.blancher@arche.fr / sid@miscmag.com

JIA 2004



# Agenda



- Les portails d'entreprise
- Problématiques de sécurité propres
  - accessibilité
  - criticité
- Solutions
  - concepts
  - architectures
- Conclusion

# Les portails d'entreprise

- Voir présentation de M. Renaud Bidou

- Intranet
- Extranet
- Internet

➔ des problématiques différentes

# Les portails d'entreprise

Les points à surveiller

- Accessibilité
- Niveau d'accès au SI de l'entreprise
- Isolation / segmentation

# Les problématiques de sécurité

Elles se situent sur deux axes :

- Accessibilité
- Type de ressources

# Accessibilité

L'accessibilité :

- Il convient de définir les population pouvant accéder aux ressources/services du portail
  - Internet : n'importe qui
  - Intranet : les population internes
  - Extranet : des partenaires identifiés

# Accessibilité

Intranet

- Population interne à l'entreprise
- Population connue et maîtrisée
- Population dans un environnement connu et maîtrisé (i.e. le SI)

➔ Il est globalement possible de gérer les accès à un Intranet sur le plan de la sécurité

# Accessibilité

Internet

- Population externe à l'entreprise
- Population inconnue
- Population évoluant dans un environnement inconnue

- ➔ Inconnu = pas de confiance
- ➔ Limitation et segmentation maximales de l'accès au ressources

# Accessibilité

Extranet

- Population externe à l'entreprise
- Population moyennement connue
- Population évoluant dans un environnement inconnu

- ➔ Le cas le plus difficile à gérer
- ➔ Difficulté à définir le niveau de confiance

# Type de ressources accessibles

Un portail met à disposition des ressources :

- Serveur HTTP
- Forum de discussion
- Listes de diffusion
- Bases de données
- Fichiers
- etc.

# Type de ressources accessibles

Ces ressources donnent accès à des informations dont le niveau de criticité varie.

Ces ressources sont disponibles sur des environnement dont le niveau de criticité varie.

# Type de ressources accessibles

Exemple :

- Le serveur HTTP publique est une ressource peu critique pour la bonne marche de l'entreprise : sa compromission n'empêche pas l'entreprise de produire.
- Ce serveur peut fournir un accès à des informations vitales (donc critiques) pour la compétitivité de l'entreprise

# Type de ressources accessibles

Pour chaque service, il faudra qualifier :

- le niveau de criticité de l'environnement hébergeant ce service
- le niveau de criticité des informations hébergées dans cet environnement

➔ Cette qualification permettra de définir le niveau d'accessibilité du service

# Type de ressources accessibles

Exemples :

- On ne laissera pas un serveur de fichiers sensibles accessible à n'importe qui
- On ne laissera pas un serveur de fichiers sensibles héberger le site Web de l'entreprise
- Etc.

# Sécurité des portails

Conclusion

- Il faut définir une classification des services
- Il faut définir une politique d'accès

- À qui s'adresse mon service ?
- Quelles sont les informations offertes ?

# Solutions de sécurité

Pour sécuriser les portails, on va utiliser des solutions des sécurité pour assurer :

- Authentification
- Confidentialité
- Intégrité
- Disponibilité

# Authentification

Brique de base

- Permet de savoir qui accède au système
- Par extension, permet de définir les droits de l'utilisateur sur le système

- ➔ Point central et incontournable

# Confidentialité

Permet de s'assurer qu'un utilisateur ne peut pas accéder à des informations qui lui sont interdites

- Contrôle d'accès
- Chiffrement

➔ Point important

# Authentification vs. Confidentialité

On ne peut pas assurer de confidentialité sans authentification :

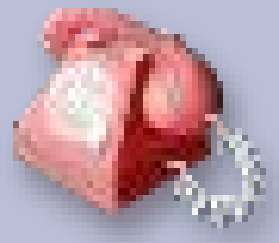
- quels droits attribue-t-on à un inconnu ?
- pourquoi chiffrer si on ne sait pas pour qui ?

# Intégrité

On doit s'assurer de l'intégrité des informations mises à disposition

- Contrôle d'accès
- Contrôle d'intégrité

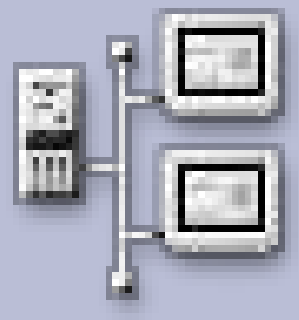
# Disponibilité



On doit assurer la disponibilité des services, particulièrement ceux qui sont critiques

- Contrôle d'accès
- Redondance
- Partage de charge

# Architectures



La mise à disposition d'un portail nécessite l'extension du SI

- L'architecture du SI doit permettre l'accueil du portail
- L'architecture doit permettre l'accès aux informations requises
- L'architecture doit isoler le portail des services auxquels il n'accède pas

# Segmentation

Principe de segmentation maximale

- Plus on isole, plus on restreint les accès
- Plus on isole, plus on assure de sécurité

➔ Principe des barrières anti-feu

# Segmentation

Principes de base

- Isoler les différents portails
- Isoler les services

- ➔ Les population qui y accèdent sont différentes
- ➔ Les informations disponibles ne sont pas les mêmes

# Segmentation

- La segmentation reste la meilleure des protection
- Elle doit s'appliquer à tous les niveaux, matériel aux relations entre applications, en passant par le réseau
- Elle s'appuie sur un contrôle d'accès fort

# Les outils

Pour assurer la sécurité, on s'appuie sur des outils classiques :

- Les applications elles-mêmes
- Des systèmes d'authentification
- Des systèmes de contrôle d'accès
- De la cryptographie
- Des filtres réseaux
- Des outils ciblés (antivirus, contrôle d'intégrité, etc.)

# Les outils

- Chaque brique peut apporter un plus en sécurité
- L'ensemble de la politique d'accès doit être implémenté (si possible) sur chaque brique du système

# Les outils

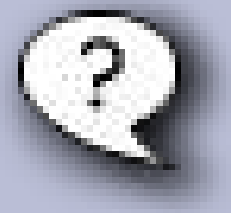
- Applications :
  - authentification, wrappers, méthodes accessibles, contrôle d'accès
- Filtres réseau :
  - firewalls sous toutes leurs formes
- Authentification
  - systèmes centralisés (Domaines, Token, etc.)
- Cryptographie
  - Essentiellement SSL/TLS
- Divers
  - antivirus, contrôle d'intégrité

# Conclusion

- Les portails sont un point d'entrée important, voire le principal point d'entrée
- Leur sécurisation est indispensable

- ➔ Prendre la sécurité en considération dès le début
- ➔ Ne surtout pas la négliger : 75% des piratages passeraient par une faille Web...

# That's all folks



Questions