MISE EN ŒUVRE DE LA SÉCURITÉ EN ENVIRONNEMENTS WINDOWS.

Agnès Benezet

agnes.benezet@UM2.fr

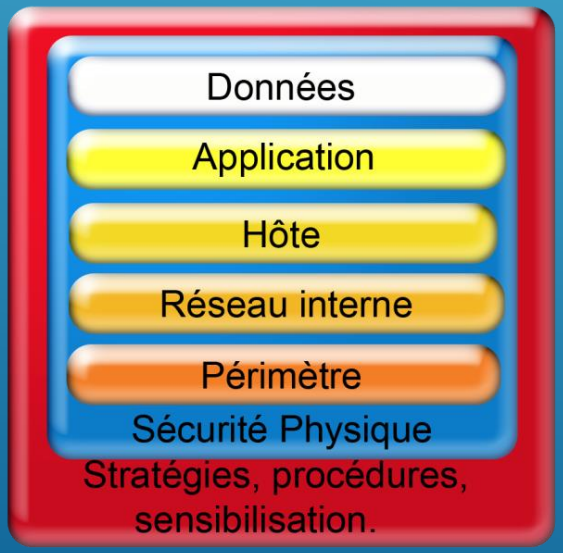
IMPORTANCE DE LA SÉCURITÉ.

STRUCTURE D'ORGANISATION DE LA SÉCURITÉ.

Approche en couche:

-Augmente les chances de détecter un intrus.

-Réduit ses chances de succès.



→ACL, Cryptage…

→ Renforcement sécurité des appli, anti-Virus/Spyware…

→Renforcement de la sécurité de l'OS, MAJ, Authentification

→Segment réseau, Wifi, IPsec

→Pare-feu, mise en quarantaine VPN…

→Restrictions /protection des d'accès, sécurisation des locaux

→Education/formation de l'usager, politique de sauvegardes des systèmes et données.

COMPOSANTS DE LA SÉCURITÉ DES POSTES CLIENTS.

COMPOSANTS DE LA SÉCURITÉ DES POSTES CLIENTS.

Mise à jour des logiciels	Appliquer la MAJ des logiciels aux systèmes i
Mot de passes	Utiliser/imposer des mots de passe sécurisés entre systèmes pour restreindre l'accès .
Protection des données	Sauvegarder et crypter les données, limiter l'accès aux données.
Sécurité des applications	Déployer, configurer et limiter l'installation des applications tierces.
Gestion des clients	Utiliser Active Directory, des modèles et des stratégies pour appliquer la sécurité.
Informatique mobile	Implémenter des stratégies et des technologies pour sécuriser l' accès à distance et l'accès sans fil. Accueil de stations visiteurs .
Périphériques externes	Stratégie de sécurisation, vaccination des postes, cryptage, proposer des d'alternatives.
Logiciel antivirus	Installer et tenir à jour un logiciel anti-virus/spyware pour empêcher l' introduction de code malveillant.
Pare-feu	Configurer des périphériques matériels ou des logiciels pour protéger le périmètre de l'entreprise .

GESTION DES MISES À JOUR LOGICIELLES

- Pour les clients et les petites entreprises (sans serveur): Windows Update.
- Pour moyenne ou grande entreprise : Rôle SUS.
- Solution de gestion des mises à jour avec niveau de contrôle et distribution de logiciels : SMS.
- Déploiements des MAJ des logiciels et modules additionnels, Acrobat, Java…

STRATEGIES DE MOTS DE PASSE

- Instruire les utilisateurs.
- Utiliser des mots de passe forts avec espace, chiffres et caractères spéciaux.
- Utiliser des mots de pase différents en fonction des ressources et protéger la liste.
- Configurer les écrans de veille et ne pas laisser une station non verrouillée . (GPO)
- Utiliser une authentification à plusieurs facteurs pour + de niveaux de sécurité.

PROTECTION DES DONNÉES.

- Utiliser EFS pour restreindre l'accès aux données.
- Signer les messages et les logiciels pour garantir leur authenticité.
- Utiliser la technologie IRM (Information Rights Management) pour protéger les informations numériques contre toute utilisation non autorisée.

SÉCURITÉ DES APPLICATIONS

Méthodes conseillées

– Apprenez aux utilisateurs à télécharger des

fichiers et à ouvrir les pièces jointes en toute sécurité

– Installez uniquement les applications dont les utilisateurs ont besoin pour leur travail

– Implémentez une stratégie pour la mise à jour des applications

L'UAC CONTRÔLE DE COMPTES UTILISATEUR

Depuis Vista et Seven

- Séparation des fonctions courantes, des actes d'administration.
- Sous XP et OS Antérieurs l' utilisateur administrateur est « administrateur » en permanence.
- Avec L'UAC, depuis Vista , il fonctionne en mode utilisateur et demande une augmentation de privilèges pour les taches d'administration.

INFORMATIQUE MOBILE

- Équipements informatiques mobile étendent le périmètres de l'entreprise
- Précautions supplémentaires :
  - Mot de passe Bios.
  - Controle d'accès distant au service IAS (Internet Authentication Service).
  - Protocole d'authentification sans fil.
  - Protection des données /cryptages disques.

INFORMATIQUE MOBILE

- Équipements informatiques mobiles entrent dans le périmètre de l'entreprise
- Précautions supplémentaires :
  - Ouverture des réseaux filaires et/ou accès wifi.
  - Contrôle de l'usage du réseau.

CLÉ USB EN ENTREPRISE.

Très pratiques pour transférer des données, les clés USB sont devenues une menace réelle pour les entreprises.

Les risques:

- Pertes de données confidentielles.
- Propagation de virus.

CLÉ USB EN ENTREPRISE.

Prévention.

- Fournir aux utilisateurs des moyens de substitution simples.
- Paramétrer les PC de manière sure
  - Inhibition des autoruns
  - Vaccination.
- Cryptage des données.
- Protection des clé par mot de passe.
- Sensibilisation de l'utilisateur.

ANTIVIRUS / ANTISPYWARES…

ANTIVIRUS / ANTISPYWARES…

- Le développement et la réactivité des menaces actuelles minimise l'efficacité des Antivirus classiques.

  Ils restent indispensables mais plus suffisants.

- Ils peuvent être associés aux antispywares pour une plus grande efficacité.

Mais au dépend des ressources de l'ordinateur.

Ne jamais installer deux antivirus sur le même poste.

DÉPLOIEMENT

Taille de l'organisation	Solution de déploiement d'antivirus
Particuliers et petites entreprises	Installer des produits antivirus sur des clients XP individuels
Organisations de petite et moyenne taille	Déploiement centralisée : Utiliser la stratégie de groupe pour déployer les logiciels antivirus
Grandes organisations	Déploiement centralisé : • Installation à l'aide de l'AD et de la stratégie de groupe • Installation et gestion à l'aide de la console d'administration du fournisseur

MISES À JOUR

- Ordinateur de bureau :
  - Les serveurs locaux stockent les fichiers de MAJ à des fins de diffusion
  - La solution idéale correspond à un modèle d'émission ou les nouvelles définitions sont immédiatement copiées vers les clients
  - Ne pas confier la MAJ aux utilisateurs.
- Ordinateur portable :
  - Utiliser les MAJ disponibles sur Internet lorsque absent du bureau.

LE PARE-FEU

MÉTHODES CONSEILLÉES

- Appliquer régulièrement les MAJ du fournisseur
- Utiliser un stratégie de déploiement centralisée
- Déployer sur les ordinateurs client des logiciels qui leur sont adaptés

UTILITÉ DES PARE FEU CLIENTS

- Pour le réseau local : protège contre les attaques automatisées
- Obligatoire pour les ordis avec connexion modem à Internet
- Obligatoire pour ordis portables connectés à Internet

MÉTHODES CONSEILLÉES

- Exiger que les utilisateurs activent leur pare-feu lorsqu'ils sont connectés au réseau.

- Utiliser des scripts pour forcer les clients distant à utiliser le pare pare-feu pour les connexions VPN.

PARE-FEU WINDOWS

- Protection de base contre les menaces en provenance d'Internet

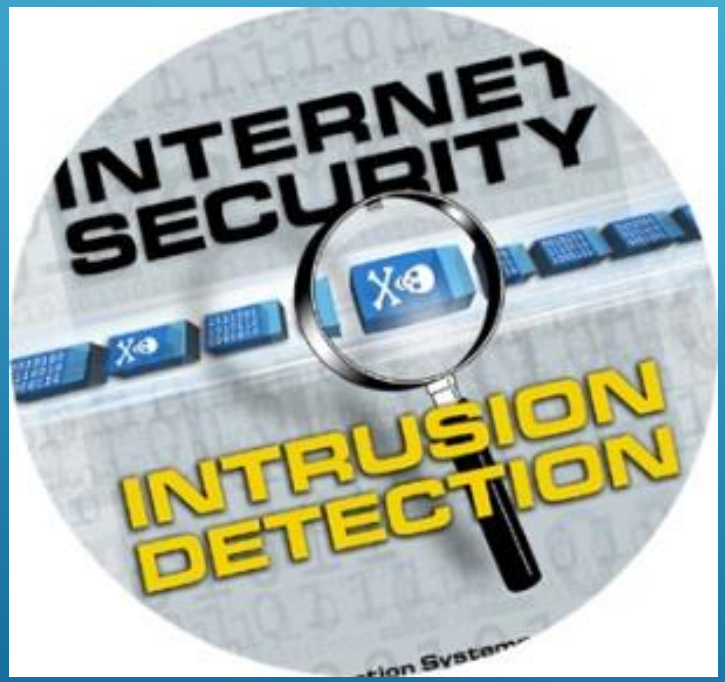
Limites :

- Problèmes de prise en charge et d'exécution de logiciels.
- Options de configuration limités.

LOGICIEL PARE FEU TIERS

- Intérêts :
  - Possibilités accrues de control du trafic entrant ET sortant
  - Fonctionnalités supplémentaires comme la détection des tentatives d'intrusion
- Inconvénients :
  - Évolutivité.
  - complexité .
  - Maintenance.

IDS / HIPS
INTRUSION DÉTECTION SYSTEM



IDS/HIPS

- Scrute le système afin de détecter toute activité suspecte ou modification.
- Détecte les accès à certaines fonctions du systèmes par des rootkits ou keyloggers.
- Intègre des vérifications au niveau du réseau. Détection des tentatives d'intrusions, des scan de ports…

IDS / HIPS

- Avantages:

- Détection comportementale indépendante des bases de données virales.
- Barrage efficace contre les rootkits.

- Inconvénients:

- Complexité de l'utilisation.
- Ressources utilisées.

POLITIQUE DE SAUVEGARDE

Recenser les besoins en sauvegarde.

Fichiers

BD

Systèmes

Messageries…

les fréquences et les spécificités.

CONCLUSIONS

Rester informé sur la sécurité

http://technet.microsoft.com/fr-fr/security/default.aspx

https://www.cert.ssi.gouv.fr/https://www.ssi.gouv.fr/

http://www.securite-informatique.gouv.fr/

Se former en permanence.