SÉCURISER MES SERVEURS MICROSOFT ET MON SI

Durée	**4 jours**	**Référence Formation**	**4-SE-SERV**

Objectifs

Réduire l'exposition aux risques
Gérer et administrer selon les meilleures pratiques
Protéger et défendre son système d'information et ses serveurs concrètement sur le terrain

Participants

Cette formation s'adresse aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement Microsoft.

Pré-requis

Une réelle connaissance informatique est nécessaire

Moyens pédagogiques

Réflexion de groupe et apports théoriques du formateur
Travail d'échange avec les participants sous forme de réunion-discussion
Utilisation de cas concrets issus de l'expérience professionnelle
Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
Alternance entre apports théoriques et exercices pratiques (en moyenne 30 à 50%)
Remise d'un support de cours

PROGRAMME

Mon réseau est-il fiable ?
- Comment analyser sa propre situation ?
- Quelques méthodes concrètes d'analyse du risque.
- Évaluer les priorités
- Mettre en perspectives les actions à mener sur le terrain par les IT

Sécurisation de l'OS du serveur :
- Version Core / Nano / Conteneur / Version avec ou sans interface graphique ? Standard ou Datacenter ?

Et la haute disponibilité dans tout ça ?
- Rappel des technologies disponibles pour l'environnement Microsoft Serveur
- Virtualisation / Cluster...

Les outils de sécurisation à ma disposition :
- Modèles d'administration
- Modèles de sécurité : SCM / SCT
- GPO
- Device Guard et Credential Guard
- Bonnes pratiques
- Normes et règles : Microsoft / Anssi
- Sources d'informations sur le Web

Maintenir son OS à jour :
- Comment obtenir et déployer les MaJ de l'OS : conseils, bonnes pratiques et outils disponibles...

Administration "Juste à temps"

CAP ÉLAN FORMATION
www.capelanformation.fr - Tél : 04.86.01.20.50
Mail : contact@capelanformation.fr
Organisme enregistré sous le N° 76 34 0908834
version 2024

- Comment utiliser l'administration "juste à temps" sur mon parc ?
- Mise en oeuvre

Forêt Bastion

- Sauvegarde et restauration
- RODC
- AD LDS

Réduction de la surface d'attaque de l'annuaire

- Normes et bonnes pratiques : Microsoft / Anssi
- Gestion des privilèges
- Délégation et administration avec privilèges minimum
- Authentification robuste et sécurisation d'accès au contrôleur de domaine
- Gestion des "droits d'utilisateurs et des services"
- Gestion des comptes d'ordinateurs et de services
- Gestion des groupes pour une meilleure sécurité

Surveillance de l'AD à la recherche d'attaques

- Les outils disponibles dans Windows : audit / powershell...
- Être alerté d'un danger potentiel
- Des outils tiers possibles

Plan de reprise ou de continuité de service en cas de compromission

- C'est arrivé ! Il me faut du temps pour réparer... Quelle est ma stratégie pendant cette période ?

Microsoft Azure et la synchronisation de l'annuaire avec le nuage

- Scénario de synchronisation AD avec Azure
- Gestion des groupes et des comptes utilisateurs
- Approche sécuritaire

Sources d'information pour la sécurisation de l'AD : normes et bonnes pratiques

- Articles Microsoft
- Articles de l'Anssi

Gestion des certificats dans Windows

- Tour d'horizon des certificats les plus utilisés : authentification / cryptage... / Rds / Exchange...
- Installation et administration de l'autorité de certification Microsoft
- Mise en œuvre concrètes des certificats

Sécurisation d'un serveur applicatif

- Applocker
- WDAC
- Le cas de messagerie Exchange
- Le cas de l'environnement RDS

Sécurisation des services réseaux

- Durcissement des protocoles utiles : Smb, Rdp, ...
- Cryptage de trafic réseau : IPSEC / SMB...
- Sécurisation du DHCP
- Sécurisation du DNS
- Pare-feu
- Serveur Radius et NPS / Contrôle d'accès réseau

Sécurisation du serveur de fichiers

- Filtrage - Quotas - Gestionnaire de rapports
- Classification de données et tâches de gestion de fichiers
- Chiffrement : EFS / BitLocker / Partage de fichiers chiffrés
- Surveillance de l'accès aux fichiers et alertes
- Gestion des permissions
- Bonnes pratiques d'administration

- Haute disponibilité : Cluster / DFS / ...

Sécurisation de la virtualisation

- Machines virtuelles blindées
- Host Guardian Service