Sécuriser mes serveurs Microsoft et mon SI

Plan de cours N° : 1301

Durée : 4 jours (28h)

PARTICIPANTS / PRE-REQUIS

Administrateurs, techniciens et responsables de parc informatique en environnement Microsoft

Connaissances générales de Windows Serveur et d'Active Directory

OBJECTIFS PEDAGOGIQUES

Réduire l'exposition aux risques. Renforcer la sécurité de son SI et de ses serveurs Windows (toutes versions). Gérer et admninistrer selon les meilleurs pratiques. Protéger et défendre son système d'information et ses serveurs concrètement sur le terrain.

MOYENS PEDAGOGIQUES

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 exercices de synthèse
Alternance entre apports théoriques et exercices pratiques (en moyenne 30 et 70%)
Remise d'un support de cours.
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS

Feuille de présence signée en demi-journée,
Evaluation des acquis tout au long de la formation,
Questionnaire de satisfaction,
Attestation de stage à chaque apprenant,
Positionnement préalable oral ou écrit,
Evaluation formative tout au long de la formation,
Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles.

MOYENS TECHNIQUES EN PRESENTIEL

Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc

MOYENS TECHNIQUES DES CLASSES A DISTANCE

A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant, suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise. L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
Les participants recevront une convocation avec lien de connexion
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par mail et par téléphone auprès de notre équipe par téléphone au 04.76.41.14.20 ou par mail à contact@atp-formation.com

ORGANISATION

Les cours ont lieu de 9h00-12h30 13h30-17h00

PROFIL FORMATEUR

Nos formateurs sont des experts dans leurs domaines d'intervention
Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

ACCESSIBILITE

Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

MISE A JOUR

10/07/2023

Sécuriser mes serveurs Microsoft et mon SI

Plan de cours N° : 1301

Durée : 4 jours (28h)

MON RESEAU EST-IL FIABLE ?

- Comment analyser sa propre situation ?
- Quelques méthodes concrètes d'analyse du risque
- Evaluer les priorités
- Mettre en perspective les actions à mener sur le terrain par les IT

SECURISATION DE L'OS DU SERVEUR

QUEL OS MICROSOFT POUR QUEL USAGE ?

ET LA HAUTE DISPONIBILITE DANS TOUT CA ?

- Rappel des technologies disponibles pour l'environnement Microsoft serveur
- Virtualisation / Cluster...

LES OUTILS DE SECURISATION A 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 A JOUR

- Comment obtenir et déployer les MAJ de l'OS : conseils, bonnes pratiques et outils disponibles

SECURISER SON ACTIVE DIRECTORY

- Analyse des risques et des attaques spécifiques au SI et à l'AD
  - Tour d'horizon des risques et des attaques les plus communes
  - Normes et bonnes pratiques proposées : Microsoft / ANSSI
- Sécuriser le contrôleur de domaine
  - Gestion de la sécurité par des contrôleurs multiples
  - Sauvegarde et Restauration
  - RODC / AD LDS

SECURISATION DES OBJETS DE L'ANNUAIRE

- Sécurisation des comptes d'utilisateurs
  - Sécurisation des comptes d'utilisateurs et de services
  - Comptes d'utilisateurs protégés
  - Comptes de services "managés"
- Gestion des comptes d'ordinateurs et délégation
  - Gestion des groupes privilégiés et sensibles
  - Gestion des droits des utilisateurs et des services
- Délégation d'administration pour protéger le SI
  - Gestion des privilèges
  - Délégation et administration avec privilèges minimum (JEA)

DESCRIPTION AVANCEE DES PROTOCOLES NTLM ET KERBEROS

- NTLM 1 et 2 : quelles failles possibles ?
- Kerberos : forces et délégation de contraintes
- Description des méthodes et outils d'attaques possibles

ANALYSE DES COMPTES PROTEGES ET SENSIBLES DE L'ACTIVE DIRECTORY

- Comptes protégés du système
- Groupes protégés du système

COMMENT SURVEILLER L'AD ET ETRE ALERTE ?

- Les outils dans Windows : audit / powershell
  - Etre alerté d'un danger potentiel
- Autres outils de centralisation des évènements et des logs
- Plan de reprise ou de continuité de service en cas de compromission

GESTION DES CERTIFICATS DANS WINDOWS

- Tour d'horizon des certificats les plus utilisés
- Installation et administration de l'autorité de certification Microsoft
- Mise en oeuvre concrète des certificats

SECURISATION DU SERVEUR DE FICHIERS

- Filtrage - Quotas - Gestionnaires 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 / ...

31, av. du Granier
38240 Meylan
Tél. 04 76 41 14 20
Fax 04 76 41 38 45

SARL au capital de 120 000€ - 390 032 050 RCS GRENOBLE
SIRET 390 032 050 00010 - APE 8559A - TVA Intracom. FR03390032050

Sécuriser mes serveurs Microsoft et mon SI

Plan de cours N° : 1301

Durée : 4 jours (28h)

SECURISATION D'UN SERVEUR APPLICATIF

- Applocker
- Restriction logicielle
- WDAC
- Le cas de messagerie Exchange
- Le cas d'environnement RDS

SECURISATION DES SERVICES RESEAUX

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

SYNTHESE SUR LA PROTECTION DE NOTRE SI

31, av. du Granier
38240 Meylan
Tél. 04 76 41 14 20
Fax 04 76 41 38 45

SARL au capital de 120 000€ - 390 032 050 RCS GRENOBLE
SIRET 390 032 050 00010 - APE 8559A - TVA Intracom. FR03390032050