ELYSIUM-Formation

Sécurisation des sauvegardes

Mise en place et sécurisation des sauvegardes

Objectifs

- Appréhender les enjeux stratégiques des sauvegardes dans un contexte de continuité d'activité.
- Identifier et différencier les divers types de sauvegardes.
- Concevoir une stratégie de sauvegarde.
- Déployer et configurer un serveur de sauvegarde sécurisé et résilient.
- Assurer la protection et la pérennité de l'infrastructure de sauvegarde face aux menaces

Contenu détaillé

Thèmes	Jour	Durée	Objectif	Remarques/Compléments d'information
Contexte				
Enjeux liés à la continuité d'activité pour l'entreprise	1	2h	Rappel	
Définitions et concepts clés (sauvegardes, DRaaS, gestion des risques, BIA, RTO/RPO, critères de sécurité, événements redoutés, ...)				
Système de management de la continuité d'activité (SMCA)				
Types de plan (PCA, PRA, PCI, PGC, etc.)				
Introduction à l'importance des sauvegardes				
Rôle des sauvegardes dans la continuité d'activité (PCA et PRA)	1	1h	Rappel	
Principales menaces : cyberattaques, erreurs humaines, sinistres physiques				
Exemples d'impacts en cas de mauvaise gestion				
Stratégies de sauvegarde				
Types de sauvegardes (complète, différentielle, incrémentielle, ...) et comparatif (avantages, inconvénients, cas d'utilisation)	1	3h	Formation	
Types de données et environnements à sauvegarder (fichiers, métadonnées, systèmes, environnements virtuel, bases de données, équipements réseaux, ...)				

Stratégie 3-2-1 : explications et mise en œuvre (3 copies, 2 supports, 1 hors site)				
Autres stratégies (3-2-1-1-0, 4-3-2)				
Mise en œuvre pratique				
Thèmes	Jour	Durée	Objectif	Remarques
Étapes de mise en œuvre d'une stratégie de sauvegarde				
Identifier et prioriser les données (en lien avec les objectifs RPO/RTO notamment)	2	2h	Formation	
Concevoir l'architecture de sauvegarde (types, outils, supports, infrastructures, ...)				
Configurer les sauvegardes selon la stratégie établie				
Assurer les MCO/MCS				
Formaliser la politique et les procédures opérationnelles				
Principes de sécurité appliqués aux sauvegardes				
Chiffrement des sauvegardes	2	3h	Formation	• Démonstrations sur des outils de sauvegarde open source. • Exercices pratiques en lien avec la journalisation et la supervision de sécurité.
Sauvegardes immuables				
Isolation logique et physique				
Contrôle d'accès et modèle Zero Trust				
Modèle de tiering				
Monitoring				
Journalisation et supervision de sécurité				
Tester et valider les sauvegardes				
Contrôle d'intégrité	2	2h	Formation	• Démonstrations sur des outils de sauvegarde open source.
Stratégie de test de restauration				
Analyse des résultats et mise à jour des processus				
Travaux pratiques inclus dans les différentes parties				

Organisation

Moyens mis à disposition

- 1 formateur expert en sécurité pour chaque session
- 1 salle de formation incluant tous les moyens nécessaires (accès Internet, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif)
- Environnement Root-Me PRO avec sélection de challenges orientés SOC/Forensique (1 licence par apprenant, accès web) => utilisé pour illustrer la partie pratique
- Lab. interne => utilisé notamment pour présenter les différents types de sauvegarde et méthodes de restauration (AD, BDD, ...)

Méthodes pédagogiques

- Horaires : accueil 9h00 ; session de formation de 9h30-17h30
- Apports théoriques et pratiques
- Exercices pratiques à base de défis
- Durée : **2 jours consécutifs en présentiel** uniquement / Lyon Part-Dieu
- Nombre d'apprenants par session : **8 maximum**
- Programme de la formation (transmis en amont de la formation)
- Support pédagogique (transmis en début de formation)
- Pré requis pour participer : un PC + une connexion Internet
- Évaluation des objectifs pédagogiques (transmise à l'issue de la formation)

Public concerné

- Equipes SSI
- Admin systèmes & réseaux
- Personnels IT en charge du déploiement des mesures de sécurité