Notes de TD Question sécu :)

Intro à l'IAM

Quels sont les éléments d'une identité numérique ? Les éléments d'une identité numérique sont un identifiant et des attributs. Il ne faut pas confondre cela avec un compte ou des éléments comme la biométrie, qui ne font pas partie de l'identité numérique.

Quels sont les types de comptes dans un système d'information ? Dans un système d'information, on distingue plusieurs types de comptes :

les comptes d'équipe,

les comptes à privilège,

les comptes individuels,

et les comptes de service. Les comptes comme les comptes industriels ou comptes nominatifs ne sont pas considérés ici.

Quel est le modèle le plus répandu de gestion des habilitations ? Le modèle le plus utilisé pour gérer les habilitations est le RBAC (Role-Based Access Control). Les autres modèles comme SBAC, UBAC ou IBAC sont moins courants ou ne s'appliquent pas ici.

Quels sont les principaux domaines de l'IAM :
- PAM
- CIAM
- IGA
- ID
- AM

La discipline CIAM correspond à la gestion des accès et des identites d'externes et notament pour les clients

La certification constitue à réviser et valider les droits

Le SSO permet de simplifier les accés, consolider les identités et donc de gérer les accés de manière centralisé

Un géstionnaire de mot de passe est un outil qui permet de générer des mot de passes fort, de stocker des mots de passes et de gérer le multi factor autentification

Un bastion est un point d'accés central pour des utilisateurs admin vers des systèmes

Cours sur les annuaire

Active Directory (AD) est un annuaire utilisé pour centraliser la gestion des utilisateurs, machines et ressources d'un réseau. C'est une grande base de données structurée.

LDAP est un protocole qui permet de consulter et modifier les données d'un annuaire comme Active Directory. Il utilise des objets définis par des classes et des attributs. Une télé, par exemple, ne serait pas un objet typique d'un annuaire AD.

Une Unité d'Organisation (UO) peut contenir d'autres UO. Cela permet de créer une hiérarchie dans l'annuaire.

Les GPO (Group Policy Objects) servent à appliquer des règles et des configurations système de façon centralisée sur les machines d'un domaine.

Les ACL (Access Control Lists) définissent les droits d'accès aux objets de l'annuaire.

Un bind est une opération qui permet de vérifier qu'un identifiant et un mot de passe sont valides pour se connecter à l'annuaire.

Le Distinguished Name (DN) indique la position exacte d'un objet dans l'arborescence de l'annuaire.

Les index accélèrent les recherches dans l'annuaire. Un annuaire est souvent plus indexé qu'une base de données classique.

cours sur la PAM (Privilage Acess Management)

Un compte a privilège est un compte dont les accés peuvent casser tout le SI.

On utilise classiquement RDP et SSH (accès aux ordinateurs à distance) pour gérer les PAM qui est d'ailleurs implémanté dans le bastion.

Dans un produit PAM on ne doit pas embarquer tous les comptes admin ou root. On ne prend que ce qu'on a besoin

Cours sur la cloud Security

Le cloud computing est une technologie moderne et efficace qui a été rendue possible par l'avènement d'Internet, des VPN et de la virtualisation qui permet d'héberger plusieurs machines virtuelles sur une machine physique.

Un déploiement cloud peut être soit publique, soit privé soit hybride (partie privée et partie publique exemple : google drive)

Différents types de Solutions cloud

IaaS = Infrastructure as a service : concrètement on a accès à la machine physique ce qui nous permet de gérer du sotckage virtuel, des capacités réseaux, des machines virtuelles voir toute autre ressource materielle. En

PaaS = Plateform as a Service : on a accès à un niveau virtualisé (OS) de la machine uniquement. Ce niveau reste très pratique si on cherche à gérer une application et les données de l'utilisateur

SaaS = Software as a service : on a seulement accès à un logiciel en ligne. Plus précisement (note pour dans 2 à 3 cours) : l'entreprise doit seulement gérer l'IAM et la sécurisation des données.

Comment mettre en place et gérer une solution Cloud, risques potentiels

On peut modifier la taille des volumes de notre service cloud grâce au principe de Scalabilité. Ceci nous permet de ne pas gaspiller de ressources et d'économiser de l'argent.

Si une entreprise veut utiliser une solution cloud chez un CSP (Cloud Provider basiquement) alors il y aura un principe de partage des responsabilités uniquement. Le client gère la configuration mais l'hébergeur reste responsable des autres sources d'attaques.

Il y a 3 domaines qui sont capitaux sur le cloud computing : - les données doivent être intègres, le système doit être auditable et ISO27001 Compliant, et il faut une compromission des données et des comptes. Ce sont les 3 domaines les plus tendus et qui peuvent poser éventuellement problème.

Il y a aussi des points tendus au niveau de la sécurité, par exemple les comptes ayant des privilèges excessifs dans le cloud et une mauvaise configuration par les clients sont à risque.

Méthodes agiles

les solutions qu'on a pour accélérer les process et être plus agile dans le dev sont le devSecOps, le Software Define Network et l'approche EaaC (Everything as a Code), concrètement on a déjà vu ces techniques en 1ere année dans le cours de méthodes agiles.

Introduction à l'IGA (Identity Governance & Administration) :

Un produit IAG a plusieurs fonctions principales attendues : gérer les processus d'habilitation, aggréger l'identité dans le SI, gérer le cycle de vie des identités et le modèle de droit Les fonctionnalités comme la sécurisation des annuaires et des comptes privilégiés n'est généralement pas prise en charge.

On définit le principe de Joiner-Moover-Leaver (JML) pour décrire les changements dans la carriere des individus d'une entreprise, et la gestion de leur accès qui change ainsi.

Dans le processus d'habilitation en particulier, il faut respecter le principe de Segregation of Duty qui permet de séparer les roles des utilisateurs.

En IGA (Identity Governance & Administration), on distingue 3 sources différentes : les golden source, les sources primaires et les sources secondaires.