Sécurité de SI

Comment optimiser la sécurité des données ?

17-10-2023

Présentée par Equipe PROLOGIC:
SGHAIER Khira
Trabelsi Dhia

1. Présentation de Prologic
2. Cadre de Mission
3. Composants de l’environnement IT
4. Vulnérabilités et Menaces
5. Risques
6. Bonnes pratiques

1
Presentation de Prologic

Présentation de la société Prologic Tunisie

Groupe Smart Tunisie

prologic IT SYSTEM BUILDER	Vente, Intégration, audit conseil et service
prologic INTERNATIONAL	Fournisseur de service IT sur l'Afrique
Smart Tunisie	Grossiste en équipements informatiques et téléphonie
SIMOP TUNISIE	Service de maintenance et d'après vente
AZUR Colors	Distributeur de machines d'impression grand format agréé HP
smart HOST	Cloud Provider

Présentation Prologic

Fruit de 38 ans d'expérience dans le conseil, la vente et le service, PROLOGIC Tunisie est aujourd'hui l'un des leaders incontestés du marché des équipements & des services informatiques.

Créée en 1985 par des experts et des passionnés de nouvelles technologies, PROLOGIC Tunisie est une société anonyme de service à haute valeur ajoutée dotée d'un capital de 3.555.000 DT

Présentation de la société Prologic Tunisie

INFRASTRUCTURES IT

Stockage, réseaux, sécurité et cybersécurité

SERVICES CLOUD

SaaS, PaaS, IaaS

PARC PC ET IMPRESSION

Solution d'impression

IT AS A SERVICE

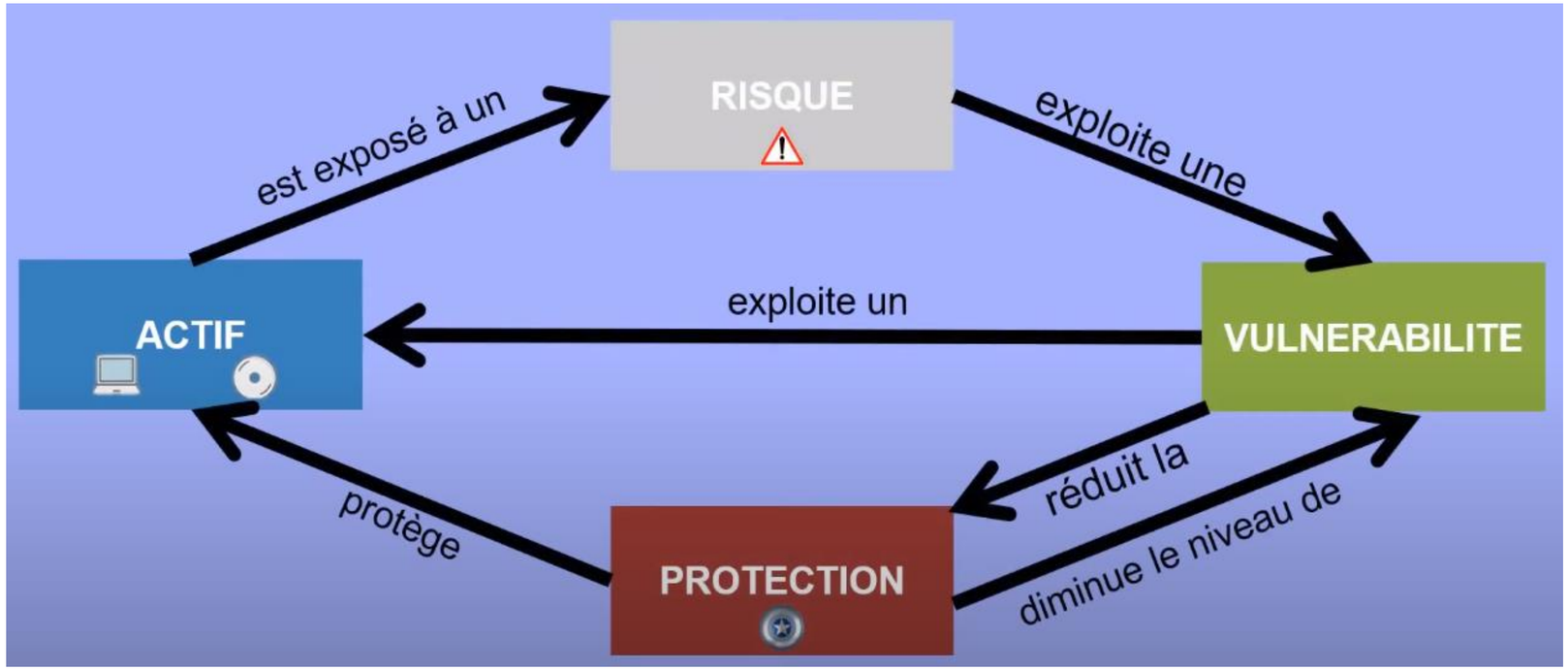
Service d'infogérance
Integration IT et Audit

2

Cadre de Mission

Cadre de Mission

Un SI est composé **d'actifs** qui sont exposés à des **risques**,
IL faut prendre des mesures de **protection** pour diminuer les **vulnérabilités**.

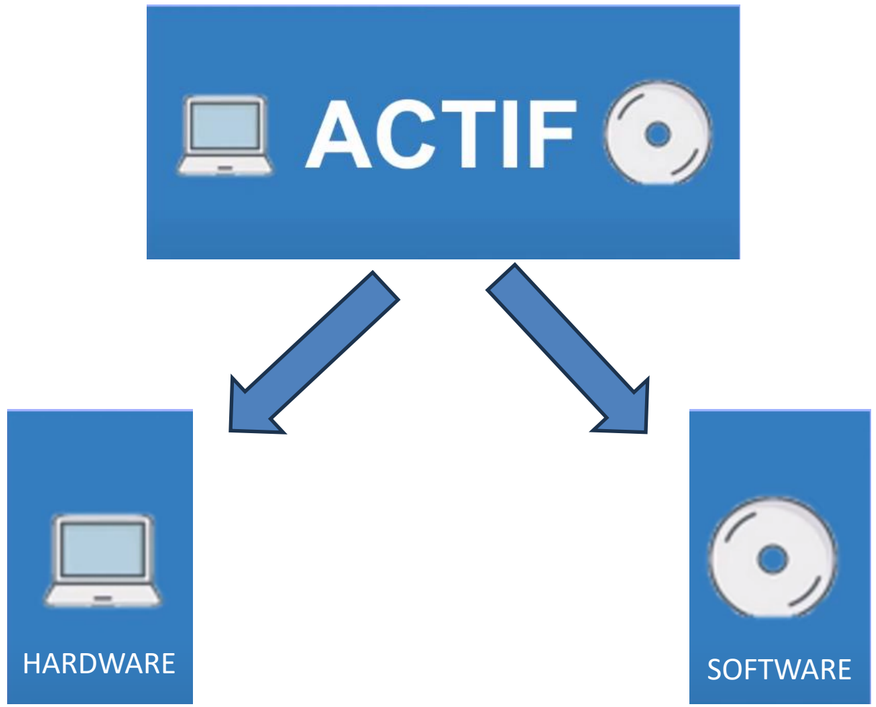


3

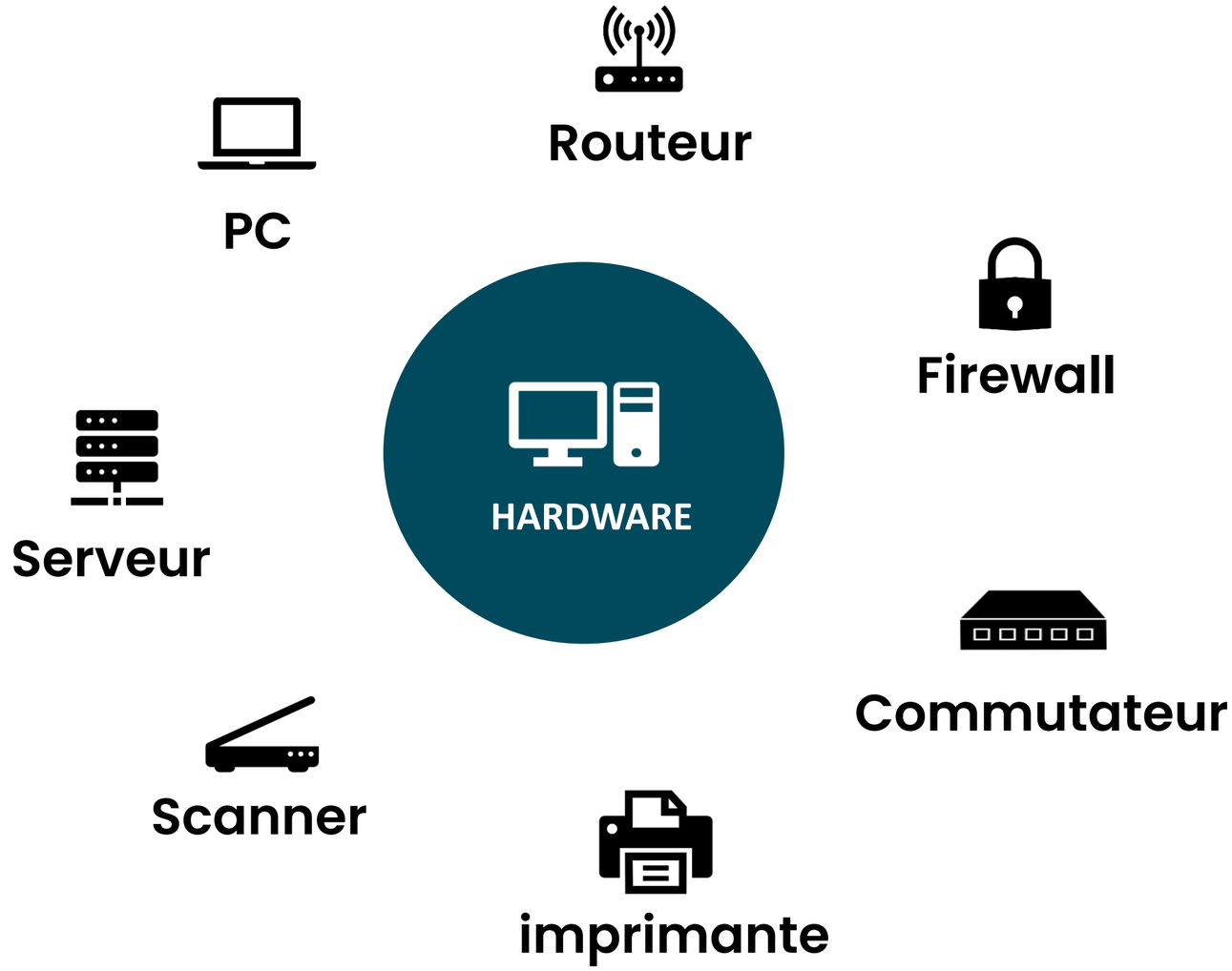
Composants de l’environnement IT

Composants de l'environnement IT

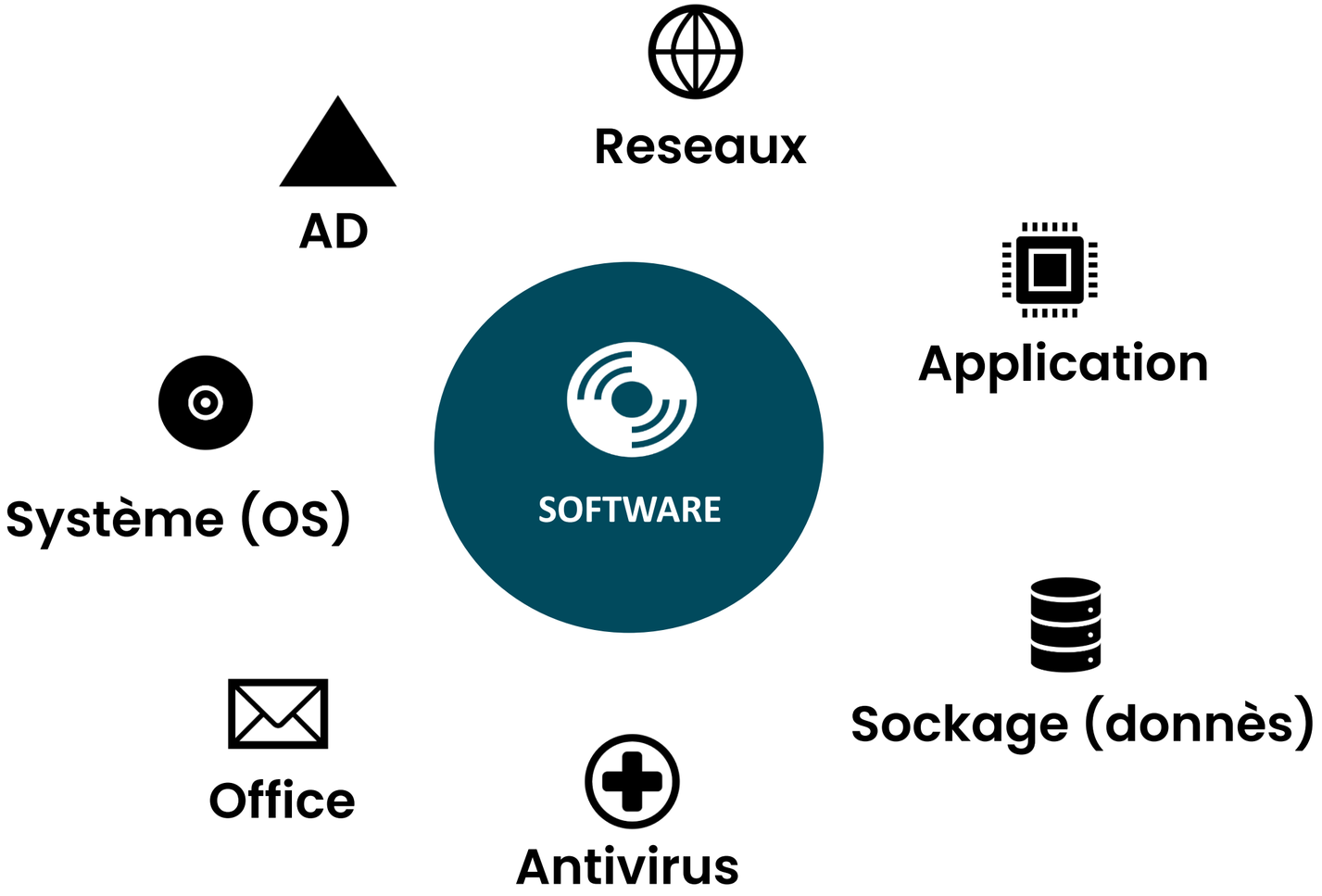
Les **matériels informatiques** (ordinateurs, imprimantes, routeur, commutateur, Firewall…) et les **logiciels** sur ces matériels.



Composants de l'environnement IT



Composants de l'environnement IT



4
Vulnérabilités et Menaces

Vulnérabilités

- Présente un defaut dans le système (dans sa construction,configuration ou conception) qui expose le système à des menaces possibles.

- Elle peut être:
  - Bugs dans les logiciels
  - Mauvaises configurations
  - Services et ports permis et non utilisés
  - Saturation de la liaison d’accès à l’internet

Vulnérabilités et Menaces

Type de vulnérabilité	Exemples
Matériel informatique	Maintenance insuffisante Stockage non protégé
Logiciel	Attribution erronée de droit d’accès Interface utilisateur compliquée
Réseau	Architecture réseau non sécurisée Point de défaillance unique
Personnel	Formation insuffisante Absence de personnel
Site (lieu)	Réseau électrique instable Site situé en zone inondable
Structure organisationnelle	Absence d’audits réguliers Absence de procédure d’accès au ressources

Menaces

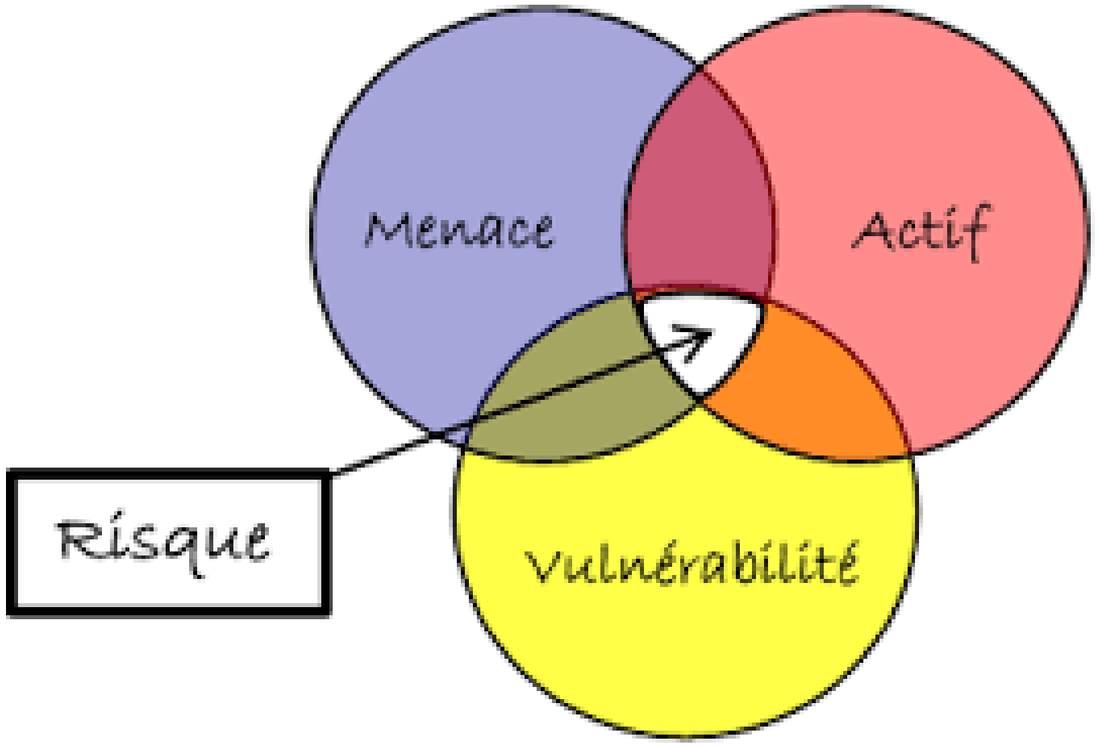
- Est un danger qui existe dans l’environnement du système indépendamment de ce dernier.
- Peut être une intention exprimée ou démontrée de nuire ou de rendre indisponible un actif.
- Les circonstances extérieures, l'erreur de la personne ou la négligence qui s'apparentent à des menaces.
- Elle peut présenter: accident, erreur, malveillance.

Vulnérabilités et Menaces

Type de menaces	Exemples
Dommage physique	Feu Dégât d'eau
Désastre naturel	Phénomène climatique Inondation
Perte de services essentiels	Panne du système de climatisation Panne électrique
Perturbations dues à des rayonnement	Rayonnements électromagnétiques Rayonnements thermiques
Compromission d'information	Vol de supports ou de documents Données provenant de source non fiable
Défaillance technique	Panne de matériel Dysfonctionnement d'un logiciel
Actions non autorisées	Utilisation non autorisée du matériel Reproduction frauduleuse de logiciel
Compromission des fonctions	Usurpation de droit

5
Risques

Risques



Le risque de sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'un actif et causent ainsi un préjudice à un organisme.

Risques

Risques = Menace x Impact x Vulnérabilité

Evènement interne ou externe pouvant affecter un SI.

Dommages financiers, perte d'image de marque, dommage réglementaires ...

Faiblesses des actifs qui peuvent être exploitées.

Une coproduction

Milan Presse

France Télévisions

Réalisation

Jacques Azam

Risques

La sécurité SI est un enjeu basé sur le critère CIDR :

Confidentialité

L’information ne peut pas être **accessible** qu'au **personne habilitées.**

Intégrité

L’information doit être transmise **sans erreurs et falsification.**

Disponibilité

Les informations doivent être **mises à disposition** en **temps** et en **heure**.

Non Répudiation

Toute action **ne peut être niée** sur les réseaux.
Le SI doit **fournir une preuve**.

Risques

Risque liée au	Exemples
Confidentialité	- Atteinte à la vie privée des clients - Usurpation d’identité - Atteinte à la sécurité du personnel
Intégrité	- SQL Injection - Erreur humaine - Erreur de transfert - Bugs et Virus
Disponibilité	- Perte d'efficacité - Interruption de service - Incapacité de fournir le service
Non Répudiation	- Attaque Man In The Middle - Ransomware

Prêt

6

Bonnes pratiques

Bonnes Pratiques

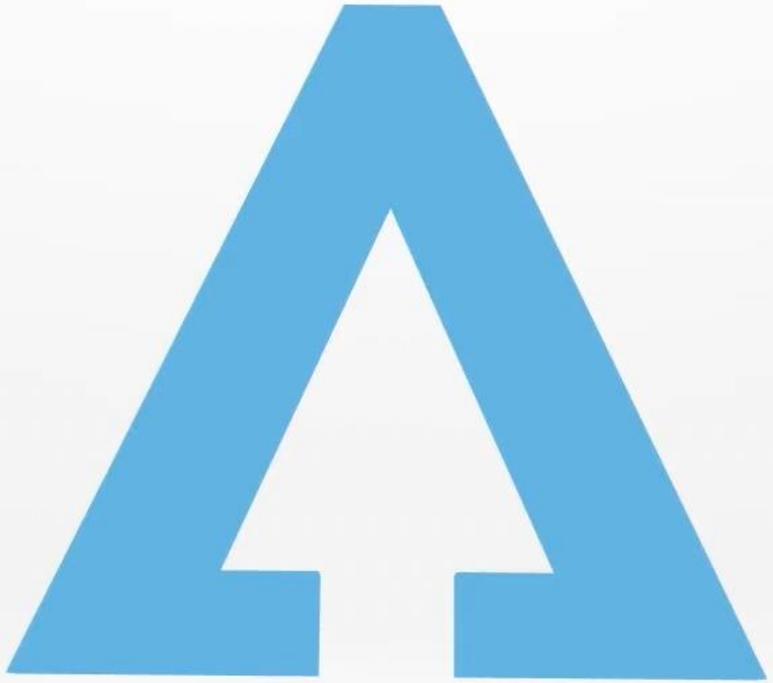
Comment assurer la sécurité physique des matériels actifs ?

- Ne pas mettre les équipements dans des environnement mouillé.
- éviter les places humides.
- Assurer la climatisation pour les serveurs et les équipements réseaux.
- Utiliser les câbles rigides et protégés.
- Offrir une électricité sécurisée et redondante.
- Protéger les ports des PCs.
- Sécuriser l’accès à la salle informatique par un contrôle d’accès (empreinte).

Bonnes Pratiques

Comment assurer la sécurité logique des matériels actifs ?

- Le système d’exploitation doit être activé et à jour.
- Les logiciels et les drivers doivent être à jour.
- Utiliser un logiciel antivirus.
- Utiliser des mots de passe forts et un gestionnaire (AD).
- Changer régulièrement votre mot de passe.
- Sauvegarder régulièrement les données.
- Éviter de cliquer sur des liens suspects.
- Nettoyer et sécuriser la boîte mail.
- Télécharger uniquement les sources sûres.
- Utiliser un pare-feu.



Bonnes Pratiques

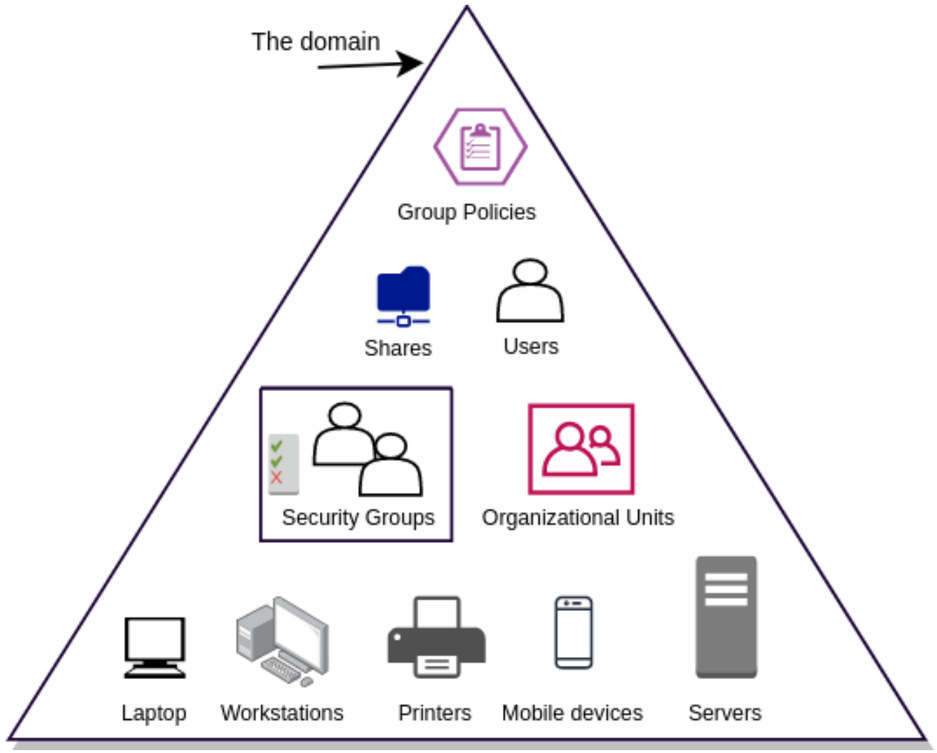
Comment assurer que le mot de passe est dans les normes ?

- Opter toujours pour un mot de passe ayant 8 caractères ou plus
- Alterner majuscules, minuscules, chiffres et caractères spéciaux
- Eviter d’utiliser des mots trop évidents comme le nom, prénom ou date de naissance
- Changer régulièrement de mot de passe.
- Activer l’authentification à deux facteurs.

Bonnes Pratiques

Quel est le rôle de l’Active Directory dans la sécurité informatique ?

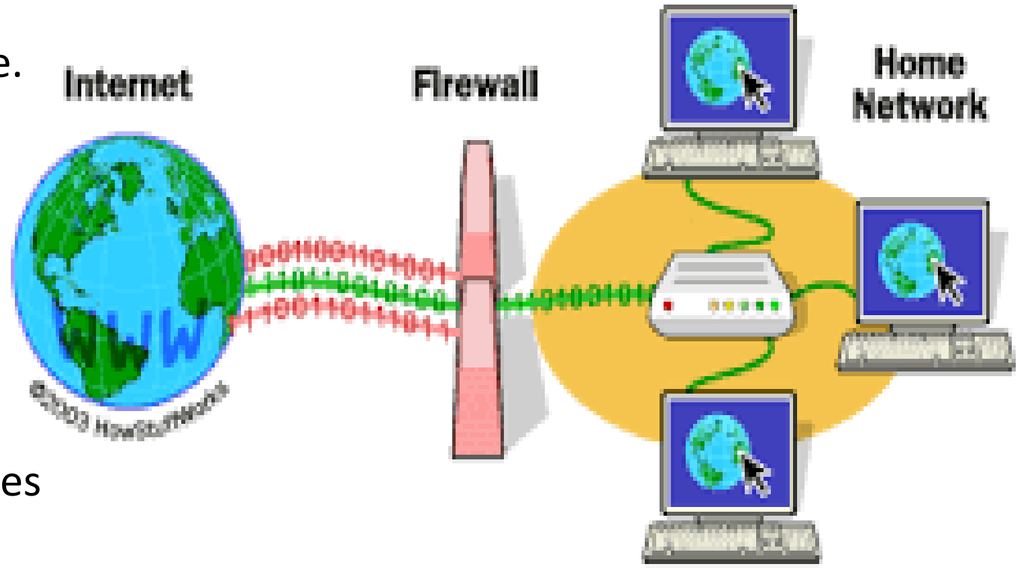
- Limiter les droits à hauts privilèges aux personnes légitimes.
- Appliquez les règles de sécurité et d’accès propres à chaque type de compte privilégié.
- Déployer des politiques de sécurité via des GPO.
- Surveiller les utilisateurs d’une manière centralisée.
- Effectuer des sauvegardes régulières de l’AD.



Bonnes Pratiques

Quel est le rôle du Firewall ?

- Filtrer le trafic entrant et sortant sur le réseau informatique.
- Protéger l’infrastructure des attaques.
- Traçabilité du flux transmis.
- Segmentation du Réseaux.
- Création des règles de sécurité.
- Bloquer les tentatives d’accès depuis l’extérieur, aux données présentes sur le réseau interne.



Bonnes Pratiques

$$\text{Risques} = \frac{\text{Menace x Impact x Vulnérabilité}}{\text{Contre-Mesure}}$$

Conclusion

Face à l’importance de la gestion de contrôle interne et de la sécurité du matériel informatique, il est important pour une entreprise de mettre en place un manuel des procédures de sécurité du matériel.

Merci pour votre attention

Equipe de Mission

Hedi Jaiet

Directeur Technique

hedi.jaiet@prologic.com.tn

Khira Sghaier

Consultante Système d’Information

khira.sghaier@prologic.com.tn

Dhia Trabelsi

Consultant Réseaux et Sécurité

dhia.trabelsi@prologic.com.tn