WILD CODE SCHOOL

Introduction à la cybersécurité

C'est quoi la cybersécurité ?

Plan

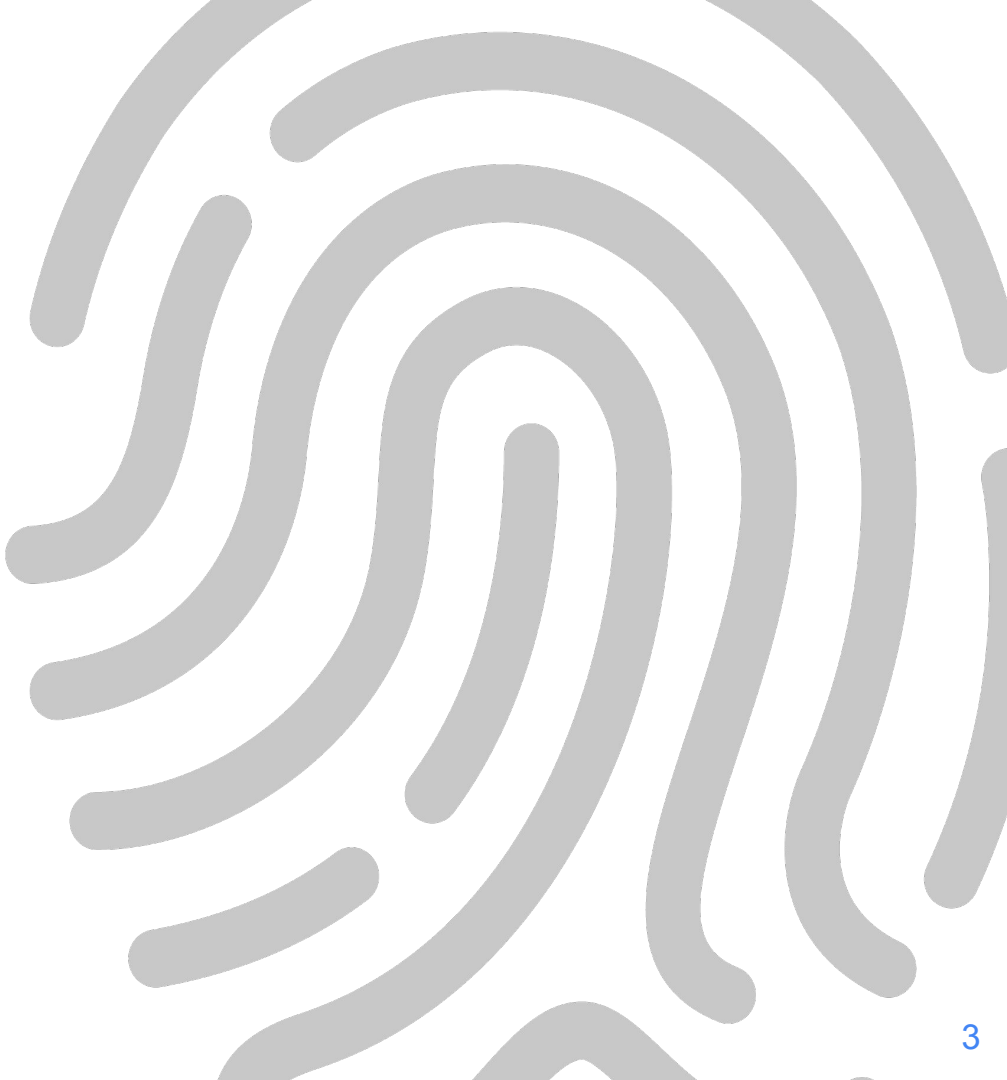
1 - Introduction

2 - Les menaces

3 - Ingénierie sociale

4 - Les logiciels malveillants

5 - Les mots de passe



WILD CODE SCHOOL

Introduction

Système d'information

Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs.
Source : WikipediA

En bref : Le SI permet et facilite la mission de l'organisation

La sécurité du SI

La sécurité du SI (ou cybersécurité) consiste à protéger le SI.

Sécurité : Protection contre les actions malveillantes
Sûreté : Protection contre les dysfonctionnements et accidents

Besoins : **D.I.C.P** (*C.I.A. in english*):

cas concret

- **Disponibilité** : service accessible aux personnes autorisées quand elles en ont besoin
- **Intégrité** : exactitude et complétude des informations, processus et moyens
- **Confidentialité** : accessible uniquement aux personnes autorisées

La preuve

Retrouver avec une confiance suffisante les circonstances des évolutions du SI

- **Traçabilité** : historique des modifications
- **Authentification** : reconnaître les utilisateurs
- **Imputabilité** : qui a fait quoi

Chaque SI a ses propres besoins D.I.C.P.

La Politique de Sécurité du SI

Concevoir une **Politique de Sécurité du Système d'Information** (PSSI)

Une **analyse de risques** :

- Cartographier le SI
- Identifier et évaluer les risques

Définir son **modèle de menace** => décider des solutions à déployer

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) est en général en charge d'établir la PSSI (*CISO - Chief Information Security Officer*)

WILD CODE SCHOOL

Les menaces

Vulnérabilité

Analyse de risques :

- **Vulnérabilité** : faiblesse de conception, réalisation, installation, configuration ou utilisation
- **Menace** : cause potentielle d'un dommage sur *tous* les éléments du SI.

Attaque : action malveillante, concrétisation d'une menace exploitant une vulnérabilité

Objectifs

Prévenir : éviter les vulnérabilités
Détecter : savoir si et quand une attaque à lieu
Réagir : décider de la réponse appropriée à l'attaque
Réparer : remettre le SI en état opérationnel
Faire évoluer la PSSI

Étude des vulnérabilités

Classement en fonction :

- des sources (niveau de compétence/moyens, interne/externe, motivations…)
- des cibles (logiciel, matériel, personnes…)
- nature des atteintes

Utilisation d'une méthodologie (ex. EBIOS RM)

WILD CODE SCHOOL

Ingénierie sociale

Définition

Ingénierie sociale (*Social Engineering*) consiste à influencer des utilisateurs légitimes pour qu'ils agissent dans l'intérêt du cybercriminel.

Via téléphone, e-mail, réseaux sociaux…

Le Hameçonnage

Le hameçonnage (*phishing*) consiste à mimer un site web (ou mail) légitime pour tenter d'obtenir des informations sensibles (identifiants et mots de passe, numéro CB…)

En général, il prend la forme d'attaque "de masse", mais le phishing ciblé existe aussi, appelé harponnage (*Spear phishing*)

Prévenir l'ingénierie sociale ?

Quelques pistes de prévention

Formation et sensibilisation des utilisateurs (tous !)

- Vérifier les URL avant connexion https://mabanque.com
- Vérifier les métadonnées
- Adopter un regard critique et vérifier les sources

Utiliser des canaux de communication sécurisés (authentifiés)

Mise en place d'antivirus (messagerie)

Pas de mauvaises pratiques (mots de passe = privé)

WILD CODE SCHOOL

Les logiciels malveillants

Malwares

Nombreux types de logiciels malveillants

Définition générale :

Programme s'installant dans un système d'information pour porter atteinte à la disponibilité, l'intégrité ou la confidentialité du système

Types de malwares

En fonction de leur nature :

- Programmes simples
- Virus (Exécutable/Macro/Boot) => contamine d'autres programmes
- Vers (Failles/Macro/Mail) => autoréplication réseau via vulnérabilités

En fonction de leur charge :

- Les bombes logiques (*Wiper*)
  - Les Rançongiciels (*Ransomware*)
- Les chevaux de troie (*Trojan*/*Keylogger*/*Backdoor*)
- Les mouchards (*Spyware*)

Robots (*Bot*/*BotNet*)

Prévenir les logiciels malveillants ?

Quelques pistes de prévention

- Déployer des antivirus à jour
- Limiter les droits (Principe de moindre privilège)
- Installer uniquement des logiciels de confiance
- Vérifier les téléchargements (empreintes et/ou signatures)
- Limiter les périphériques d'entrée

WILD CODE SCHOOL

Les mots de passe

Mot de passe

Définition :

Moyen d'authentification se basant sur la connaissance d'une information secrète

On parle en général de mots de passe ou de phrases de passe (long)

Mot de passe vs Clé

Choisi vs aléatoire

En mémoire vs stocké

Limites intuitive :

Vérification => connaissance du mot de passe

Les mauvaises pratiques

Les attaques

- Force brute
- Attaque par dictionnaire
- Capture en clair
- Enregistreur de frappes
- Ingénierie sociale
- ...

La force brute

Principe :

Essayer toutes les possibilités

Problème :

0 Caractère => 1 essai

4 chiffres => 10 000 essais (0,01 s à 1 essai/µs)

8 caractères alphanumériques => 62^8 = 2 x 10^{14} (≅7 ans)

16 caractères ASCII => 95^{16} (≅10^{18} ans)

Contres-mesures :

Augmenter la complexité des mots de passe (taille, variété)

Limiter ou ralentir les tentatives

Les attaques par dictionnaire

Principe :

Mots de passe plus probables

Ex : 123456, 123456789, qwerty, password…

Contres-mesures :

Limiter ou ralentir les tentatives

Interdire les mots de passe courants

Capture en clair

Principe :

Lire le mot de passe
Quand il est transmis => écoute réseau
Où il est stocké => BDD, système de fichiers, post-it...
Quand il est tapé

Contres-mesures :

Chiffrer les communications réseau => TLS
Ne pas stocker les mots de passe
Sécuriser son poste de travail
Ne pas taper ses mots de passe en public

Quelques constats

Multiplication des services =>
réutilisation massive des mots de passe

Mots de passe sont un compromis
complexité - mémorisable

Base de données "sera" compromise
voir : actualité des fuites de données

Sondage : vos pratiques
Qui n'utilise **que** des mots de passe **longs**, **aléatoires** et **uniques** ?

Ne pas stocker les mots de passe

Principe :

Fonctions de hachage disponibles
Comparer l'empreinte ≍ Comparer le message
=> Stockage d'empreintes

Problème résolu ?

Même mot de passe = même empreinte
Création de tables mot de passe => empreintes pré-calculées (tables arc-en-ciel)

Hachage de mot de passe

Salage :

Ajout d'un sel (aléatoire mais non secret) au moment du calcul de l'empreinte

Mots de passe identiques => Empreintes différentes

Stockage : empreinte + sel

Calcul coûteux

Pour contrer les pré-calculs

Avoir un calcul d'empreinte long

Bons candidats :

yescrypt, scrypt, bcrypt, argon2

Gestionnaire de mots de passe

Stockage chiffré d'information de connexion

- Clé dérivée d'une phrase de passe

Générateur de mots de passe

Auto remplissage

Plus d'info : page WikipediA

Conclusion

- Notions de PSSI, D.I.C.P, vulnérabilité, menace, attaque
- Différentes menaces classique
- Question des mots de passe