

Introduction

Posons le décor !

Le contexte

- Multiplication des systèmes d'informations,
- Démocratisation des outils informatiques,
- Généralisation des accès à Internet,
- Complexité des architectures (privées, publiques, cloud, hybrides,...),
- Diversification de la nature des données (financières, médicales, technologiques,...),
- Professionnalisations des acteurs malveillants,
- ...

Objectifs et motivations des attaques

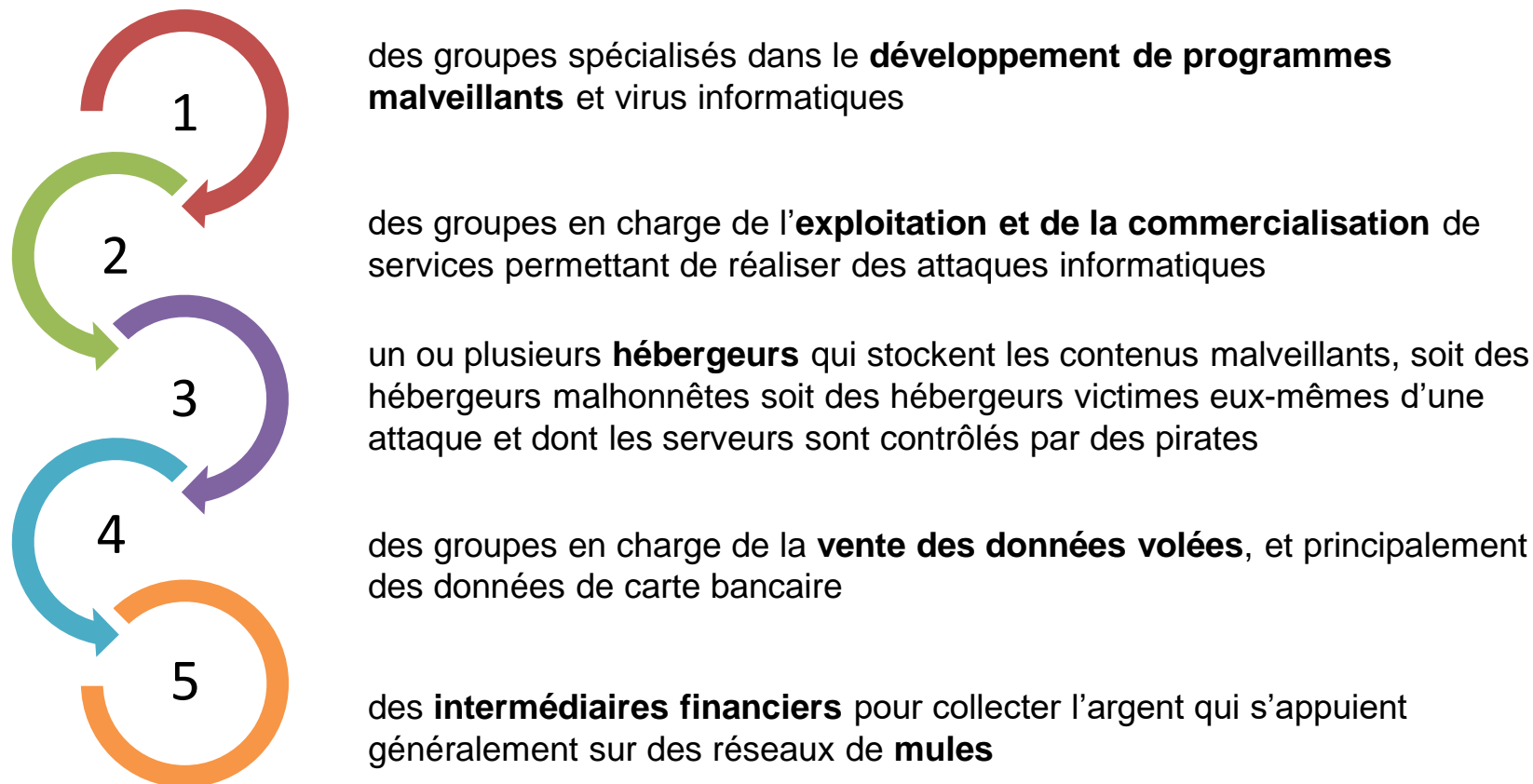
- Vol d'information,
- Modification d'information,
- Prise de contrôle d'un système,
- Destruction du système ou de ses informations,
- Non disponibilité d'un service,
- Préparation d'une attaque plus massive,
- ...
- Pour des raisons politiques, idéologiques, financières, « ludiques »,...

Les moments de vie d'une attaque: méthodologie du hacker.

- 1) collecte de l'information
- 2) intrusion
- 3) en option : garantir un accès plus facile dans le futur
- 4) reconnaissance interne
- 5) en option : mouvement
- 6) exécution de l'action voulue
- 7) en option : couvrir les traces

Zoom sur la motivation financière

La nouvelle économie de la cybercriminalité



- Quelques chiffres pour illustrer le marché de la cybercriminalité...

de **2 à 10 \$**

le prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays et des plafonds

5 \$

le tarif moyen de location pour 1 heure d'un **botnet**, système permettant de saturer un site internet

2.399 \$

le prix de commercialisation du **malware** « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 \$)

Quelques acteurs et un vocabulaire à s'approprier

- Black Hats,
- Grey Hats,
- White Hats,
- Script Kiddies,
- Cyber terroriste,
- Hacktiviste,
- Crackers,
- Carder,
- Phreaker,
- RSSI,
- ...

Les différents types d'attaques

- Virus,
- Worms / Vers
- Chevaux de Troie,
- Spywares,
- Adwares / logiciel publicitaire ou publiciels,
- Ransomware
- Spam,
- Phishing / Hameçonnage
- DoS / DDoS,
- MitM,
- ...

- Virus: programme malveillant capable de se propager et de contaminer d'autres programmes (ou parfois d'autres données) → il a besoin d'un « hôte ».
- Ver: programme malveillant autonome qui n'a pas besoin du programme hôte pour se répliquer.

(*) Différencier de façon plus exhaustive virus et ver nécessiterait un plus long développement.

- Cheval de Troie: programme malveillant caché à l'intérieur d'un autre programme à l'allure légitime. L'exécution de ce dernier provoquant celle du programme malveillant.
- Spyware: logiciel « espion », récolte des informations sur le système ou sur son utilisation (à l'insu du propriétaire) et les transmet à l'agresseur.
- Adware: s'infiltré dans votre ordinateur pour vous forcer à regarder des publicités (ou des publicités spécifiques) que vous ne regarderiez normalement pas, ou forcent secrètement votre ordinateur à se rendre sur des sites web ciblés pour augmenter le nombre de vues, et générer ainsi des revenus publicitaires mal acquis.

- Spam: Le spam, parfois traduit en français par « pourriel » ou « pollurriel », contractions respectives des termes poubelle et pollution avec le terme courriel, désigne tout courrier non sollicité par le destinataire. Généralement, il s'agit de messages envoyés à des fins publicitaires ou malveillantes.
- Ransomware: chiffre vos données et vous demande de l'argent pour les déchiffrer.
- Phishing: Les e-mails ou les sites web de phishing tentent d'inciter l'utilisateur à fournir ses données légitimes de connexion, en se faisant passer pour un site web authentique ou un administrateur que l'utilisateur connaît.

- DoS – DDoS: Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.
- MitM: Man in the middle: individu malveillant interceptant les échanges entre deux parties légitimes → accède ou modifie les données échangées.
- ...

<!> Cette classification est très théorique et les attaques actuelles ne limitent pas leur appartenance à une seule catégorie stricte <!>

Ex: WannaCry présente les caractéristiques d'un ver (autoréplication) + celles du ransomware (chiffrement des données).

Définition du SI

A qui s'adresse cet exposé ?

- Prioritairement aux personnes qui seront en charge d'un système d'information dans une entreprise ou une institution.
- Certains principes exposés peuvent toutefois aussi être utiles pour un particulier.

Que voulons nous gérer/protéger ?

Un système d'information

ou

Un système informatique

Système informatique

- Le terme *système informatique* a une connotation trop technique et ne reflète pas les diverses réalités que nous allons rencontrer.
- Passons donc au SI: Système d'information

Partie 1

Le système d'information

Système d'information

- Définition de wikipédia:

« 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 ordinateur. Il s'agit d'un système socio-technique composé de deux sous-systèmes, l'un **social** et l'autre **technique**. Le sous-système social est composé de la structure organisationnelle et des personnes liées au SI. Le sous-système technique est composé des technologies (hardware, software et équipements de télécommunication) et des processus d'affaires concernés par le SI. »

→ 3 composantes + 4 actions primaires = 1 rôle

- 3 composantes:
 - Technique (Hardware + Software),
 - Humaine,
 - Information.
- 4 actions primaires:
 - Collecter,
 - Stocker,
 - Traiter,
 - Distribuer/diffuser l'information.
- 1 rôle :
 - Permettre l'existence de solutions technologiques au **service** du métier et des processus qui composent ce métier : les **processus métiers**.

Définition de service

*« Un **service** est un moyen de fournir de la valeur aux clients en facilitant les résultats qu'ils souhaitent obtenir sans porter toute la responsabilité des coûts et des risques. »*

Avec clients = véritables clients ou collaborateurs internes

P.ex. dans une école, la mise à disposition d'une plateforme d'encodage des notes et d'envoi des bulletins aux élèves est un service.

Définition de processus.

« Un **processus** est une suite structurée d'actions ou d'activités inter-reliées qui permet d'atteindre un ou plusieurs but. » Source : Jean-Luc Baud, ITIL 4, Ed ENI.

→ Une processus métier est un processus qui permet d'atteindre un but propre à un métier. p.ex. dans une école, l'inscription d'un nouvel élève/étudiant.

Comment concilier processus métier et service ?

Via la mise à disposition d'**applications métier**: des briques logicielles du SI spécifiques aux processus métier.

Exemples:

- CRM (*Customer Relationship Management*) : gestion des relations avec les clients.
- ERP (*Enterprise Resources Planning*) : gestion du pilotage de l'entreprise(RH, paie, ventes, production, logistique, comptabilité,...).
- SRM (*Supplier RelationShip Management*) : gestion des relations avec les fournisseurs
- PDM, PLM, ... selon les activités de l'organisation.

A ce stade, on peut dire que :

Un SI = un ensemble de technologies + des actions humaines, permettant l'existence de services, qui ne sont généralement rien d'autre que des applications métier (ou assimilées), mises à disposition des clients.

Ces applications métiers aident les travailleurs dans l'accomplissement de leurs processus métier (leur job en somme...).

On dit que cette aide apporte de la **valeur** au métier.

Le terme « **aide** » aurait sans doute été mieux choisi mais il est moins *business*. 😊

Et puis comme aide \approx aide à la productivité \approx accroissement des valeurs, autant aller droit au but... et conserver « valeur ».

Au cœur du SI : l'information

L'information constitue la composante centrale du SI car elle permet à l'organisation de :

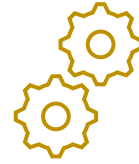
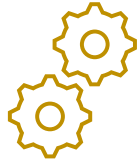
- Prendre des décisions,
- Réaliser ses activités,
- Créer de la valeur,
- Répondre à des obligations légales,
- Définir les actions futures,
- ...

Finalement...

Si le SI veut vraiment aider (\approx apporter de la valeur à) l'organisation, il doit permettre les 4 actions primaires liées à l'information:

- La collecte,
- Le stockage,
- Le traitement,
- La diffusion.

Action primaire 1 : collecter l'information + la mettre en forme



Information → Collecte → Mise en forme selon une structure préétablie → SI → ...

- La structure préétablie étant essentiellement
 - des fichiers (Word, Excel, PDF, ...)
 - ou des bases de données (DB SQL, Access, Oracle,...).
- Les sources d'information peuvent être :
 - Interne : information générée par l'organisation/entreprise elle-même (p.ex. l'enseignant qui insère ses documents dans le SI d'une école, c.-à-d. le dépôt sur la plateforme).
 - Externe : information générée par des parties prenantes en relation avec l'organisation.

Remarque

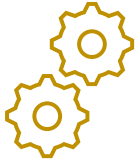
La collecte peut être couteuse, surtout en cas d'intervention humaine (encodage) → concevoir des stratégies pour diminuer ces coûts (standardisation des informations encodées, automatisation, délégation de la tâche,...).

Exemple d'une inscription d'un étudiant : *le secrétariat encode vs le scan de la Carte d'id.*

<!> ces entrées d'informations dans le SI sont déjà des sources de risques → la sécurité débute dès cette première étape <!>

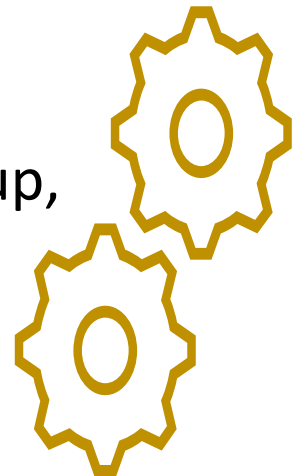
Action primaire 2 : stocker l'information

Information → Collecte → Mise en forme selon une structure préétablie → SI →
Stockage → ...



Enregistrement de l'information sur un support numérique

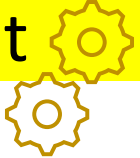
- + ajout de métadonnées,
- + des mécanismes de protection contre les actions malveillantes,
- + des mécanismes de *retour en arrière* vers un état $T - x$ de l'information: le backup,
- + des mécanismes de mise à disposition simultanée depuis différents points de stockage = la synchronisation,
- + la gestion de l'archivage,
- + la gestion de la destruction de l'information.



Où stocker l'information ?

- Localement :
 - Sur des supports classiques: disques durs, NAS, bandes, DVD,...
 - Sur une agrégation de plusieurs supports physiques organisés en *réseaux de stockage* : SAN (Storage Area Network).
- A l'extérieur :
 - Dans un *cloud*, géré par un prestataire de service.

Action primaire 3 : Traiter l'information

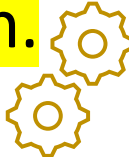
Information → Collecte → Mise en forme selon une structure préétablie
→ SI → Stockage → **Traitement**  → ...

Le traitement peut être:

- Une simple consultation,
- Une organisation : structurer l'information selon des critères spécifiques,
- Une mise à jour,
- Une production de nouvelle(s) information(s) à partir d'information(s) existante(s).

Action primaire 4 : Diffuser l'information

Information → Collecte → Mise en forme selon une structure préétablie → SI → Stockage → Traitement → **Diffusion.**



- Au(x) bon(s) destinataire(s),
- Au bon moment,
- Sous la bonne forme = directement exploitable.