



Initiation à la cyber sécurité

Initiation à la cyber sécurité

Plan du module

- 1. Les enjeux de la sécurité des S.I.**
- 2. Les besoins de sécurité**
- 3. Notions de vulnérabilité, menace, attaque**
- 4. Panorama de quelques menaces**

1. Les enjeux de la sécurité des S.I.

- a) Préambule**
- b) Les enjeux**
- c) Pourquoi les pirates s'intéressent aux S.I.?**
- d) La nouvelle économie de la cybercriminalité**
- e) Les impacts sur la vie privée**
- f) Les infrastructures critiques**
- g) Quelques exemples d'attaques**

a. Préambule

Système d'Information (S.I.)

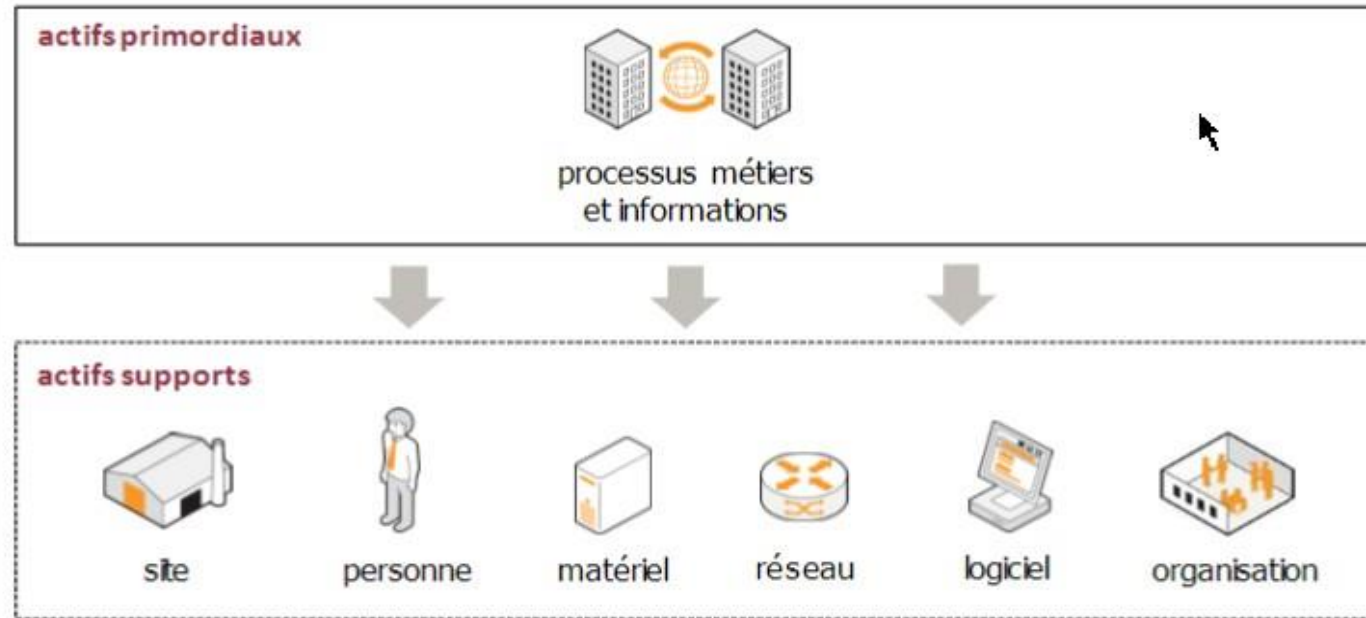
- Ensemble des ressources destinées à collecter, classer, stocker, gérer, diffuser les informations au sein d'une organisation
- Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

Le S.I. doit permettre et faciliter la mission de l'organisation.

1. Les enjeux de la sécurité des S.I.

a. Préambule

- Le système d'information d'une organisation contient un ensemble d'actifs:



ISO/IEC 27005:2008

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

1. Les enjeux de la sécurité des S.I.

b. Les enjeux.

La sécurité a pour objectif de réduire les risques pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations...

La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire:

- Elle **contribue à la qualité de service que les utilisateurs** sont en droit d'attendre
- Elle **garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

1. Les enjeux de la sécurité des S.I.

- b. Les enjeux



1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

Les motivations évoluent

- Années 80 et 90: beaucoup de bidouilleurs enthousiastes
- De nos jours: majoritairement des actions organisées et réfléchies
- Cyber délinquance

Les individus attirés par l'appât du gain

- Les «hacktivistes»
- Motivation politique, religieuse, etc.
- Les concurrents directs de l'organisation visée
- Les fonctionnaires au service d'un état
- Les mercenaires agissant pour le compte de commanditaires
- ...

1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus?

Gains financiers(accès à de l'information, puis monétisation et revente)

- Utilisateurs, emails
- Organisation interne de l'entreprise
- Fichiers clients
- Mots de passe, N° de comptes bancaires, cartes bancaires

Utilisation de ressources (puis revente ou mise à disposition en tant que «service»)

- Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
- Zombies(botnets)

Chantage

- Dénî de service
- Modifications des données

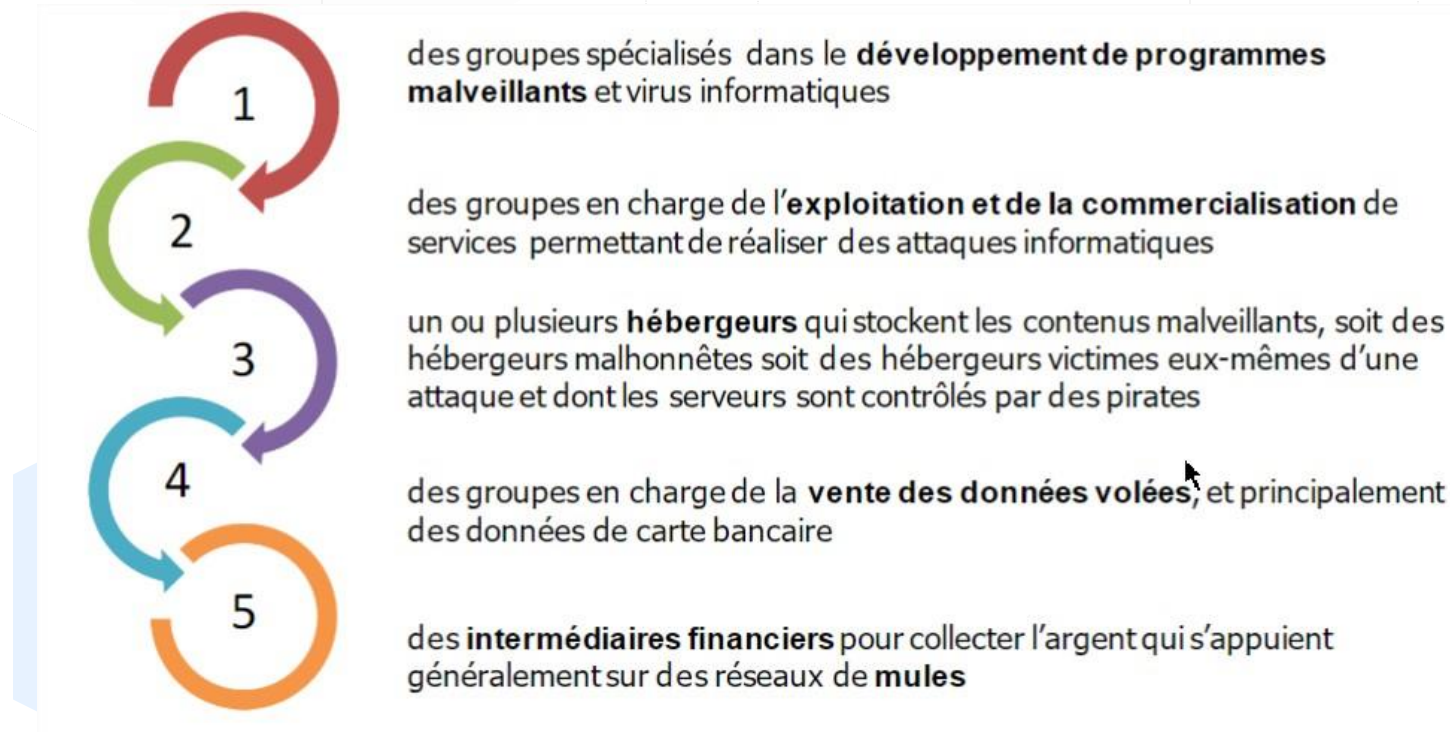
Espionnage

- Industriel/concurrentiel
- Étatique
- ...

1. Les enjeux de la sécurité des S.I.

d. La nouvelle économie de la cybercriminalité

Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs



1. Les enjeux de la sécurité des S.I.

d. 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 \$)

1. Les enjeux de la sécurité des S.I.

e. Les impacts de la cybercriminalité sur la vie privée (quelques exemples)

- **Impact sur l'image/ le caractère/ la vie privée**
 - Diffamation de caractère
 - Divulgateion d'informations personnelles
 - Harcèlement/cyber-bullying
- **Usurpation d'identité**
 - «Vol» et réutilisation de logins/mots d'identification pour effectuer des actions au nom de la victime
- **Perte définitive de données**
 - Malware récents (rançongiciel): données chiffrées contre rançon
 - Connexion frauduleuse à un compte «cloud» et suppression malveillante de l'ensemble des données
- **Impacts financiers**
 - N° carte bancaire usurpé et réutilisé pour des achats en ligne
 - Chantage (divulgateion de photos ou d'informations compromettantes sinon paiement d'une rançon)

1. Les enjeux de la sécurité des S.I.

e. Les impacts de la cybercriminalité sur les infrastructures critiques

- Infrastructures critiques = un ensemble d'organisations parmi les secteurs d'activité suivants, et que l'État français considère comme étant tellement critiques pour la nation que des mesures de sécurité particulières doivent s'appliquer
 - Secteurs étatiques: civil, justice, militaire...
 - Secteurs de la protection des citoyens: santé, gestion de l'eau, alimentation
 - Secteurs de la vie économique et sociale: énergie, communication, électronique, audiovisuel, information, transports, finances, industrie.
- Ces organisations sont classées comme **Opérateur d'Importance Vitale**(OIV).
La liste exacte est classifiée(donc non disponible au public).

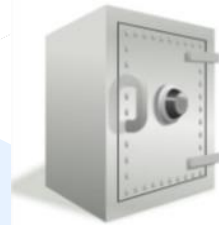
2. Les besoins de sécurité

- a) Introduction aux critères DIC**
- b) Besoin de sécurité: «Preuve»**
- c) Différences entre sureté et sécurité**
- d) Exemple d'évaluation DICP**
- e) Mécanisme de sécurité pour atteindre les besoins DICP**

2. Les besoins de sécurité

a. Introduction aux critères DIC

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé?
- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C



Disponibilité

Propriété d'**accessibilité au moment voulu** des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité

Propriété d'**exactitude et de complétude** des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

Confidentialité

Propriété des biens de **n'être accessibles qu'aux personnes autorisées**

2. Les besoins de sécurité

b. Besoin de sécurité: «Preuve»

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé?
- 1 critère complémentaire est souvent associé au D.I.C.

Bien à
protéger



Preuve

Propriété d'un bien permettant de retrouver, avec une **confiance suffisante**, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe
Notamment :

La **traçabilité** des actions menées
L'**authentification** des utilisateurs
L'**imputabilité** du responsable de l'action effectuée

2. Les besoins de sécurité

c. Différences entre sûreté et sécurité

«Sûreté» et «Sécurité» ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements...

Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage...*

*Certaines de ces parades seront présentées dans ce cours

2. Les besoins de sécurité

c. Différences entre sûreté et sécurité

Sûreté: ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.

Sécurité: ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

Le périmètre de chacune des 2 notions n'est pas si clairement délimité dans la réalité: dans le cas de la voiture connectée on cherchera la sécurité et la sûreté.




2. Les besoins de sécurité

d. Exemple d'évaluation DICP


Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

L'expression du besoin attendu peut-être d'origine:

- **Interne**: inhérente au métier de l'entreprise
- **Externe**: issue des contraintes légales qui pèsent sur les biens de l'entreprise.



Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible

 Le bien bénéficie d'un niveau de sécurité adéquat

2. Les besoins de sécurité

d. Exemple d'évaluation DICP

- Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- Exemple avec un site institutionnel simple(statique) d'une entreprise qui souhaite promouvoir ses services sur internet:

Disponibilité = **Très fort** ✓

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaître ses services au public

Intégrité = **Très fort** ✓

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)



Serveur web

Confidentialité = **Faible** ✓

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = **Faible** ✓

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

2. Les besoins de sécurité

- **e. Mécanismes de sécurité pour atteindre les besoins DICP**
- Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie:

		D	I	C	P
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓	
Cryptographie	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓	✓
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓		✓	
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dûment habilitées		✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

		D	I	C	P
Capacité d'audit	Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.	✓	✓	✓	✓
Clauses contractuelles avec les partenaires	Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients	✓	✓	✓	✓
Formation et sensibilisation	Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I. Diffusion des bonnes pratiques de sécurité. Le cours actuel en est une illustration !	✓	✓	✓	✓
Certains de ces mécanismes seront présentés dans le cadre cette sensibilisation à la cybersécurité					

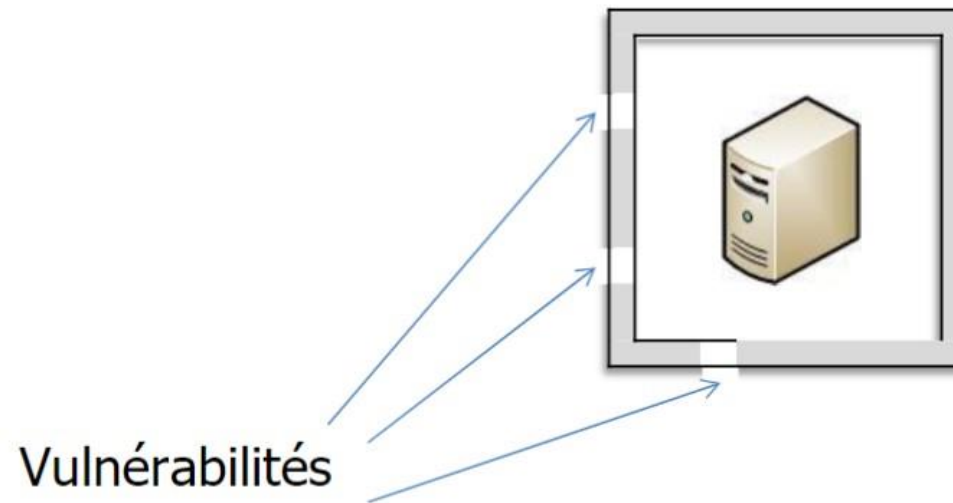
3. Notions de vulnérabilité, menace, attaque

- a) Notion de «Vulnérabilité»**
- b) Notion de «Menace»**
- c) Notion d'«Attaque»**
- d) Exemple de vulnérabilité lors de la conception d'une application**
- e) Illustration d'un usage normal de l'application vulnérable**
- f) Illustration de l'exploitation de la vulnérabilité présente dans l'application**

3. Notions de vulnérabilité, menace, attaque

a. Notion de «Vulnérabilité»

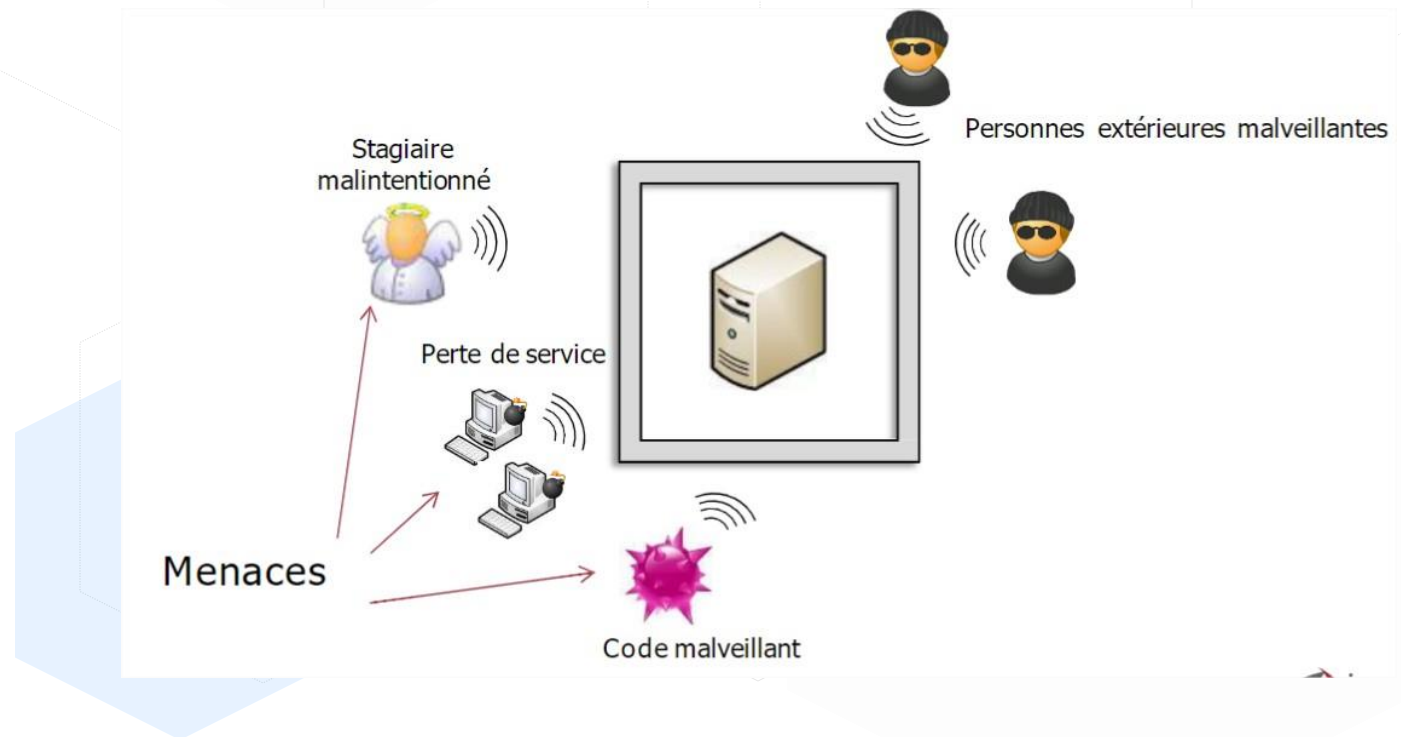
- Vulnérabilité
- Faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



3. Notions de vulnérabilité, menace, attaque

b. Notion de «Menace»

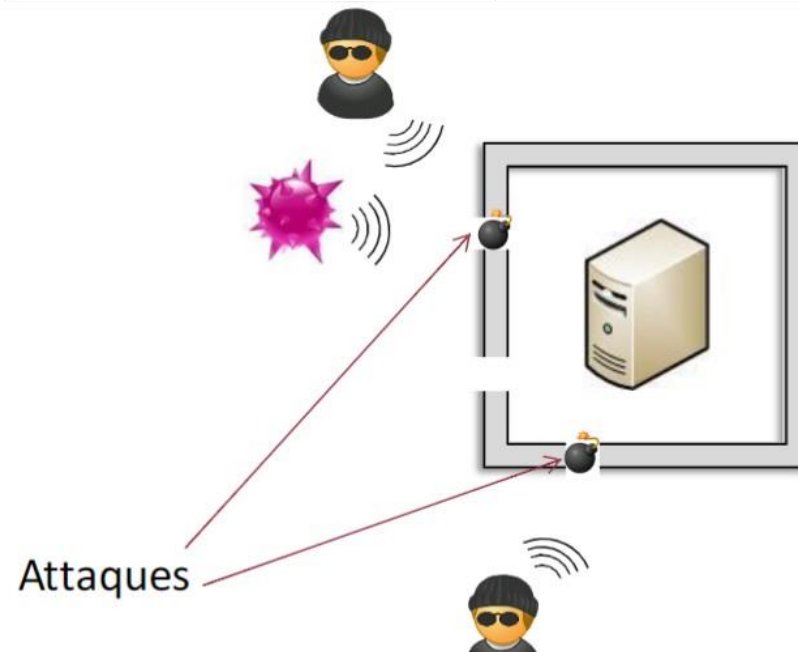
- Menace
- Cause potentielle d'un incident, qui pourrait entraîner des dommages sur un bien si cette menace se concrétisait.



3. Notions de vulnérabilité, menace, attaque

c. Notion d'«Attaque»

- **Attaque**
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité**.



3. Notions de vulnérabilité, menace, attaque

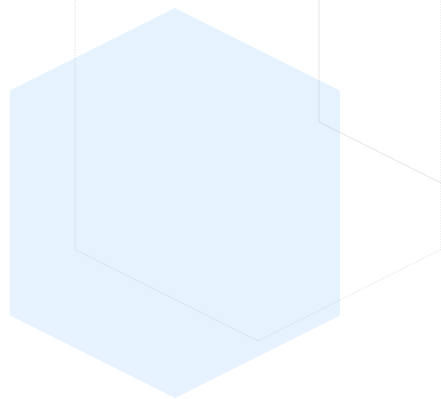
c. Notion d'«Attaque»

- Attaque

- Une attaque ne peut donc avoir lieu(et réussir) que si le bien est affecté par une vulnérabilité.

Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maîtriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

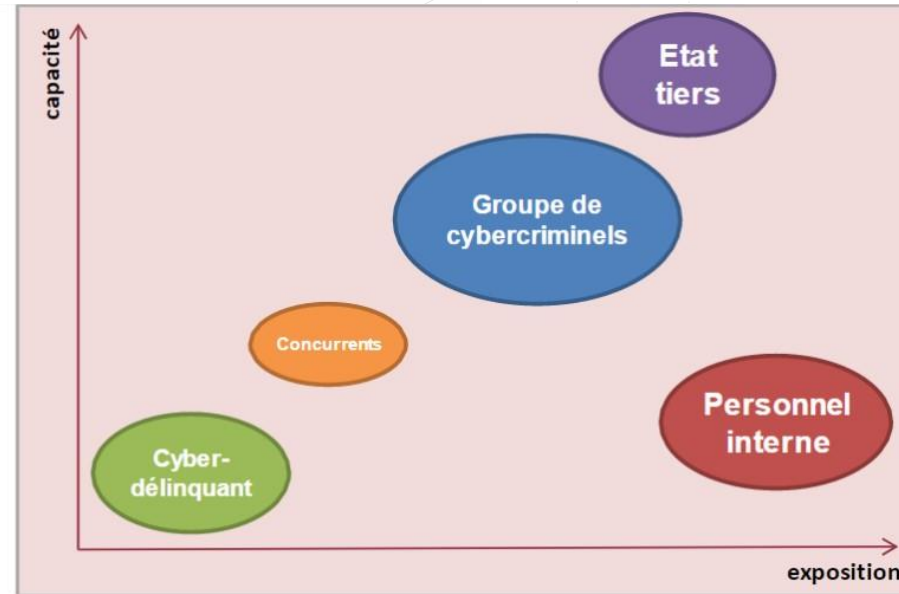


4. Panorama de quelques menaces

- a) Les sources potentielles de menaces**
- b) Hameçonnage & ingénierie sociale**
- c) Déroulement d'une attaque avancée**
- d) Violation d'accès non-autorisé**
- e) Fraude interne**
- f) Virus informatique**
- g) Déni de service Distribué(DDoS)**
- h) Illustration d'un réseau de botnets**

4. Panorama de quelques menaces

a. Sources potentielles de menaces



Capacité
degré d'expertise et ressources
de la source de menaces

Exposition
opportunités et intérêts de la
source de menaces

Exemple d'une cartographie des principales sources de menaces
qui pèsent sur un S.I.

Attention: cette cartographie doit être individualisée à chaque organisation car toutes les organisations ne font pas face aux mêmes menaces.

Exemple: le S.I. d'une administration d'état ne fait pas face aux mêmes menaces que le S.I. d'un e-commerce ou d'une université.

4. Panorama de quelques menaces

b. Hameçonnage & ingénierie sociale

L'hameçonnage(anglais: «**phishing**») constitue une «**attaque de masse**» qui vise à abuser de la «**naïveté**» des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire...

- 1- Réception d'un mail utilisant le logo et les couleurs de l'entreprise
- 2- Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe
- 3- Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant
- 4- Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site



4. Panorama de quelques menaces

b. Hameçonnage & ingénierie sociale

L'«**ingénierie sociale**» constitue une «**attaque ciblée**» qui vise à abuser de la «**naïveté**» des employés de l'entreprise:

- Pour dérober directement des informations confidentielles, ou
- Pour introduire des logiciels malveillants dans le système d'information de la banque



par téléphone



par réseaux
sociaux



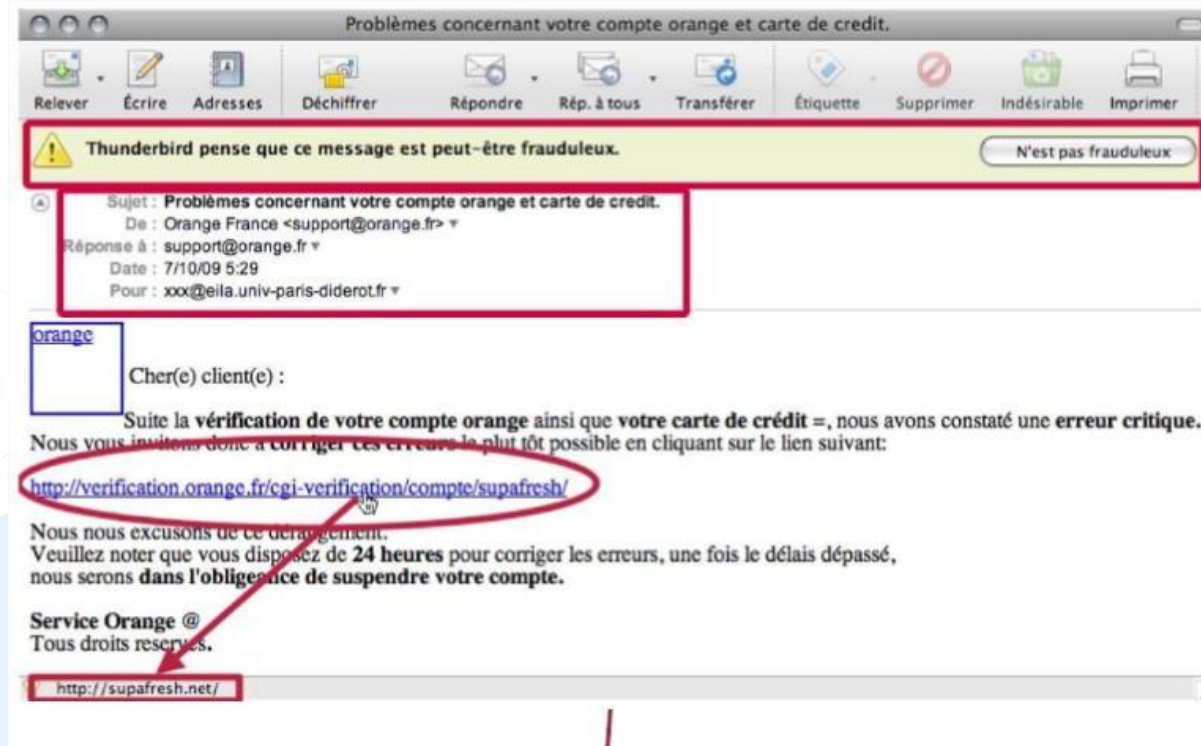
par e-mail

Les scénarios d'ingénierie sociale sont illimités, avec pour seules limites l'imagination des attaquants et la naïveté des victimes...

4. Panorama de quelques menaces

b. Hameçonnage & ingénierie sociale

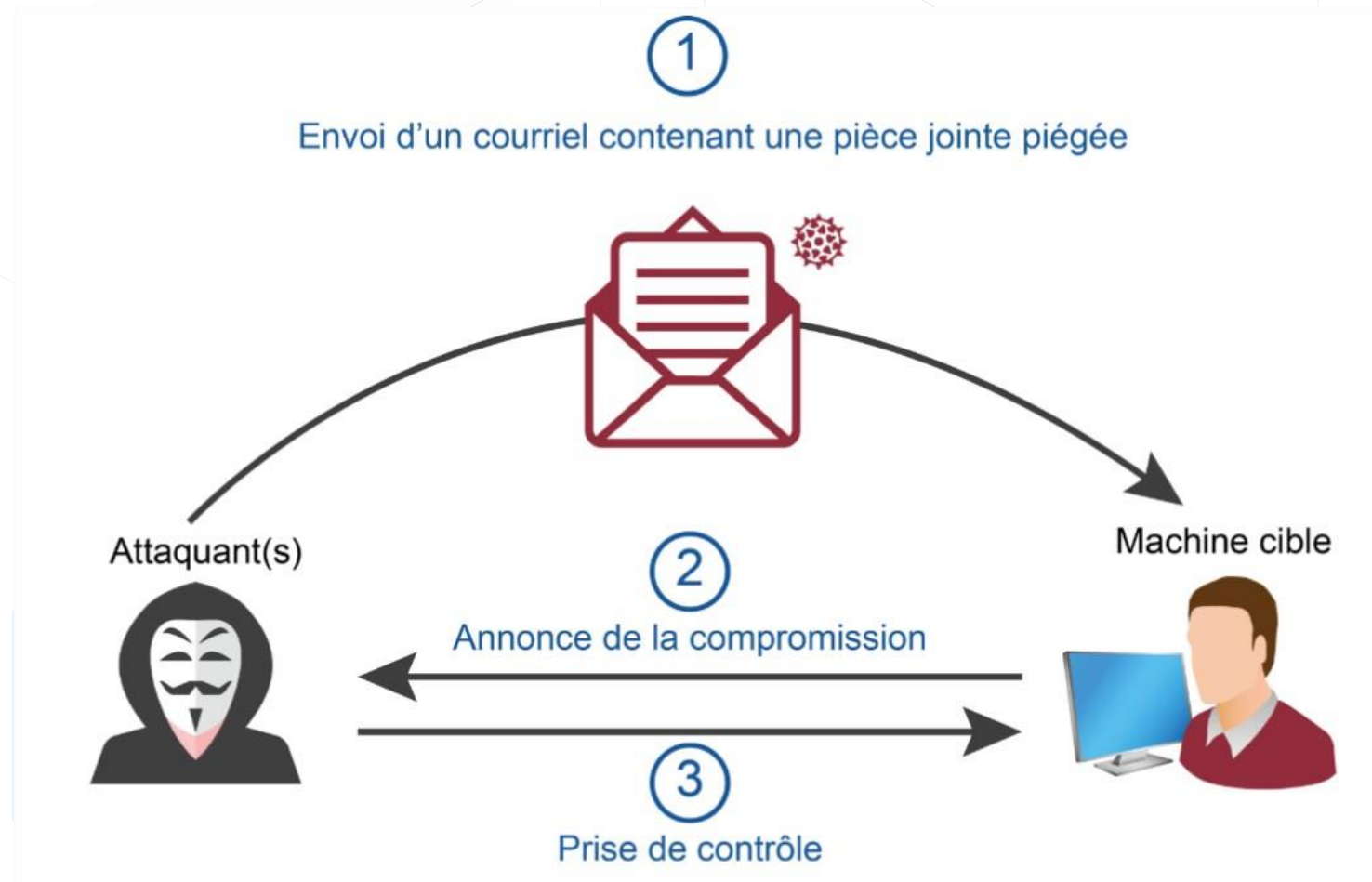
Exemple de **phishing** ciblant les employés d'un grand groupe français...



Ce lien pointe en fait vers un site frauduleux, et non pas vers un serveur légitime de l'entreprise

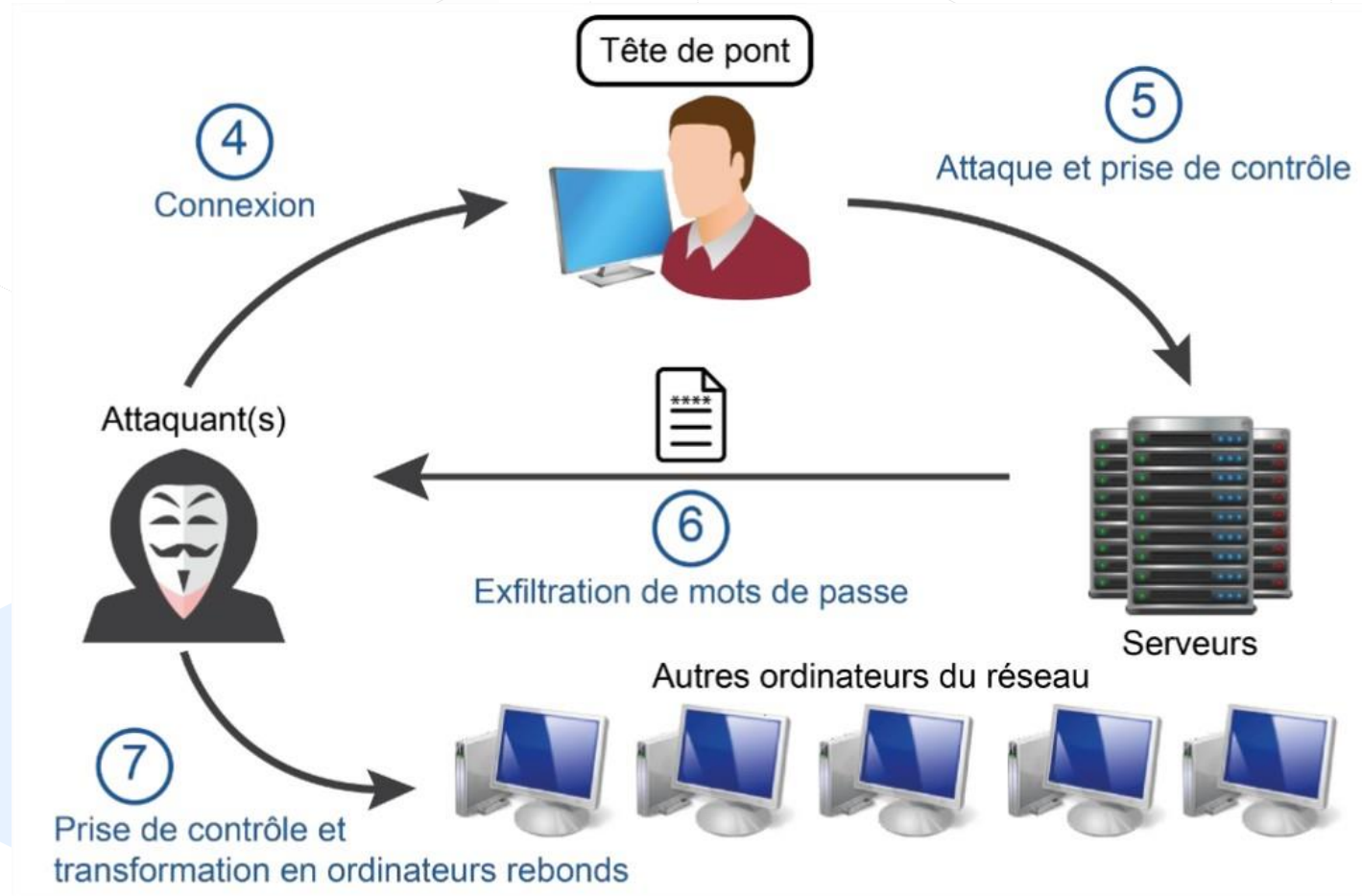
4. Panorama de quelques menaces

c. Déroulement d'une attaque avancée



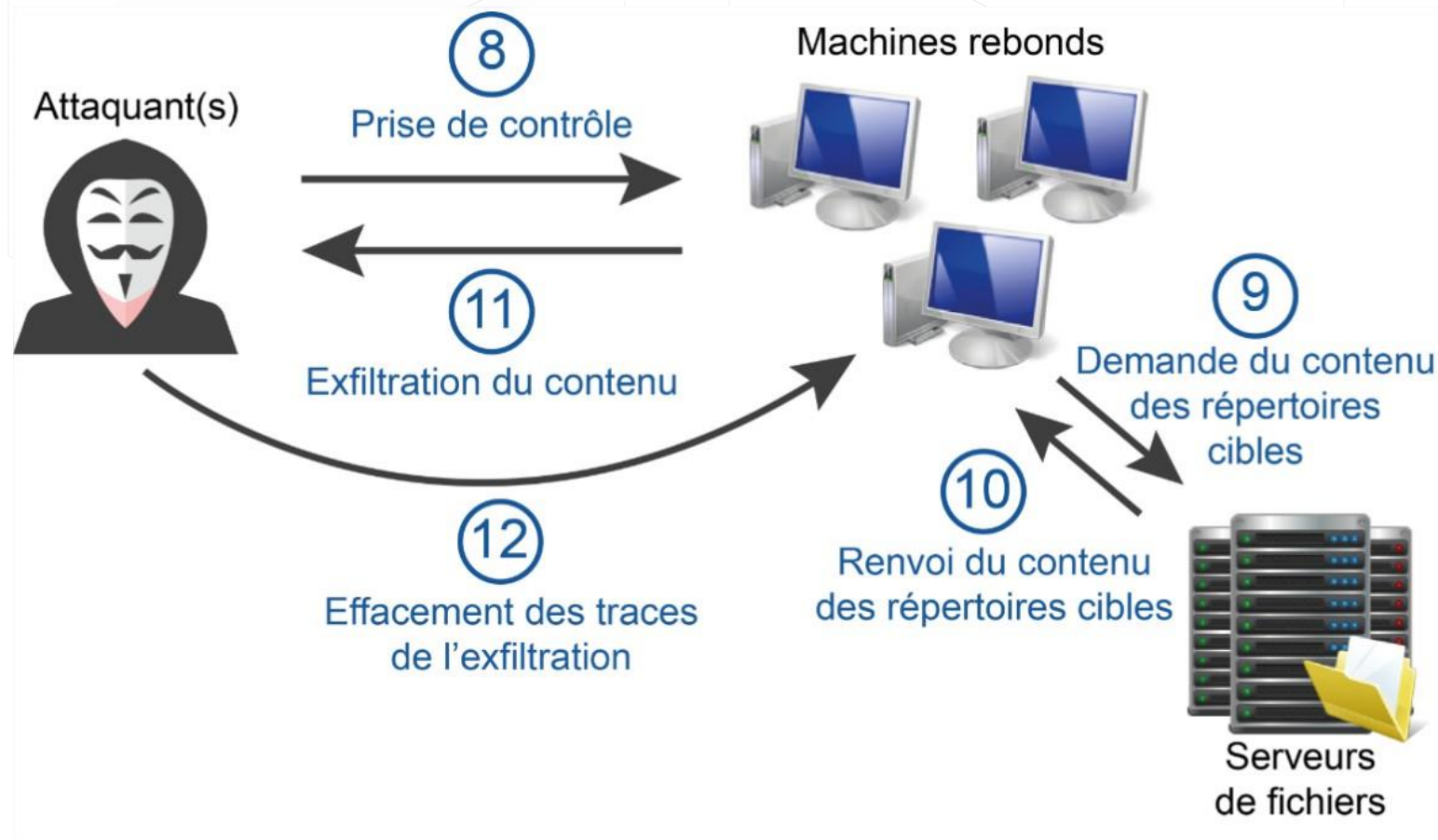
4. Panorama de quelques menaces

c. Déroulement d'une attaque avancée



4. Panorama de quelques menaces

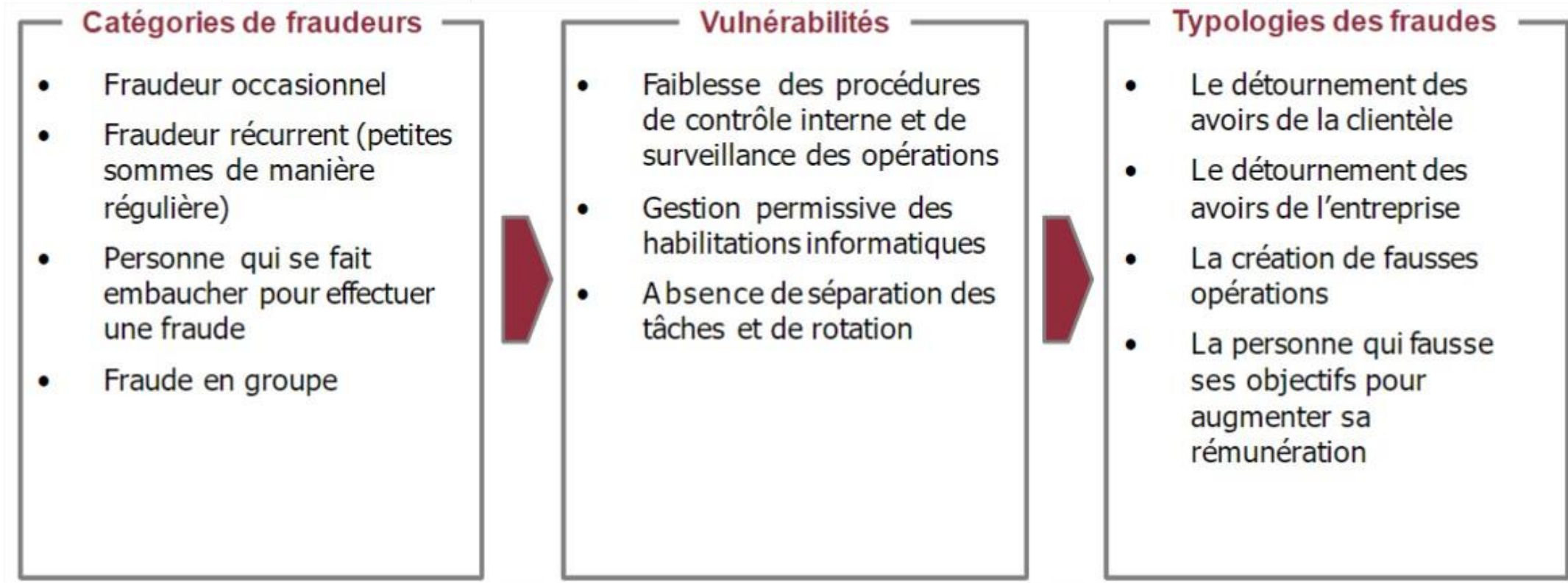
c. Déroulement d'une attaque avancée



4. Panorama de quelques menaces

d. Fraude interne

La **fraude interne** est un «sujet tabou» pour les entreprises, mais un véritable sujet d'importance!



4. Panorama de quelques menaces

e. Violation d'accès non autorisé: mots de passe faibles

Des mots de passe simples ou faibles(notamment sans caractères spéciaux comme «!» ou «_» et des chiffres) permettent entre-autre à des attaquants de mener les actions suivantes:

- Utiliser des **scripts automatiques** pour tester un login **avec tous les mots de passe couramment utilisés(issus d'un dictionnaire)**;
- Utiliser des **outils pour tenter de «casser» le mot de passe**. Ces outils sont très efficaces dans le cadre de mots de passe simples, et sont beaucoup moins efficaces dans le cas de mots de passe longs et complexes.
- Réflexion sur l'utilisation des mots de passe: les mots de passe constituent une faiblesse significative pour la cybersécurité. En effet, **les êtres humains n'ont pas la capacité de mémoriser de nombreux mots de passe**, complexes, différents pour chaque application, etc.
- Pour cette raison, **d'autres moyens d'authentification émergent**, de façon à libérer les individus des problématiques des mots de passe. Quelques exemples: la biométrie, les tokens USB, les matrices papier, la vérification via un code SMS, les «one time password», etc.

4. Panorama de quelques menaces

e. Violation d'accès non autorisé: intrusion

Les intrusions informatiques constituent des «attaques ciblées» qui exploitent une ou des vulnérabilité(s) technique(s) pour dérober des informations confidentielles (ex.: mots de passe, carte bancaire...) ou prendre le contrôle des serveurs ou postes de travail

Depuis le réseau Internet sur les ressources exposées: sites institutionnels, services de e-commerce, services d'accès distant, service de messagerie, etc.

Depuis le réseau interne sur l'Active Directory ou les applications sensibles internes

Quelques chiffres issus de tests d'intrusion menés sur de nombreux S.I.:

80% des domaines Active Directory sont compromis en 2 heures

75% des domaines Active Directory contiennent au moins 1 compte privilégié avec un mot de passe trivial

50% des entreprises sont affectées par un défaut de cloisonnement de ses réseaux

80% des tests d'intrusion ne sont pas détectés par les équipes IT

Sources : tests d'intrusion Orange Consulting 2012-2013

4. Panorama de quelques menaces

f. Virus informatique

Les **virus informatiques** constituent des «**attaques massives**» qui tendent...

- A devenir de plus en plus ciblés sur un **secteur d'activité**(télécommunication, banque, défense, énergie, etc...)
- A devenir de plus en plus **sophistiqués** et **furtifs**



Quelques virus récents et médiatiques : Citadel, Flame, Stuxnet, Duqu, Conficker, Zeus, Shamoon (Aramco)...

Les principaux vecteurs d'infection...

- **Message** avec pièce-jointe
- Support amovible (**clé USB...**)
- **Site Web** malveillant ou piratés
- **Partages réseaux** ouverts, systèmes vulnérables...



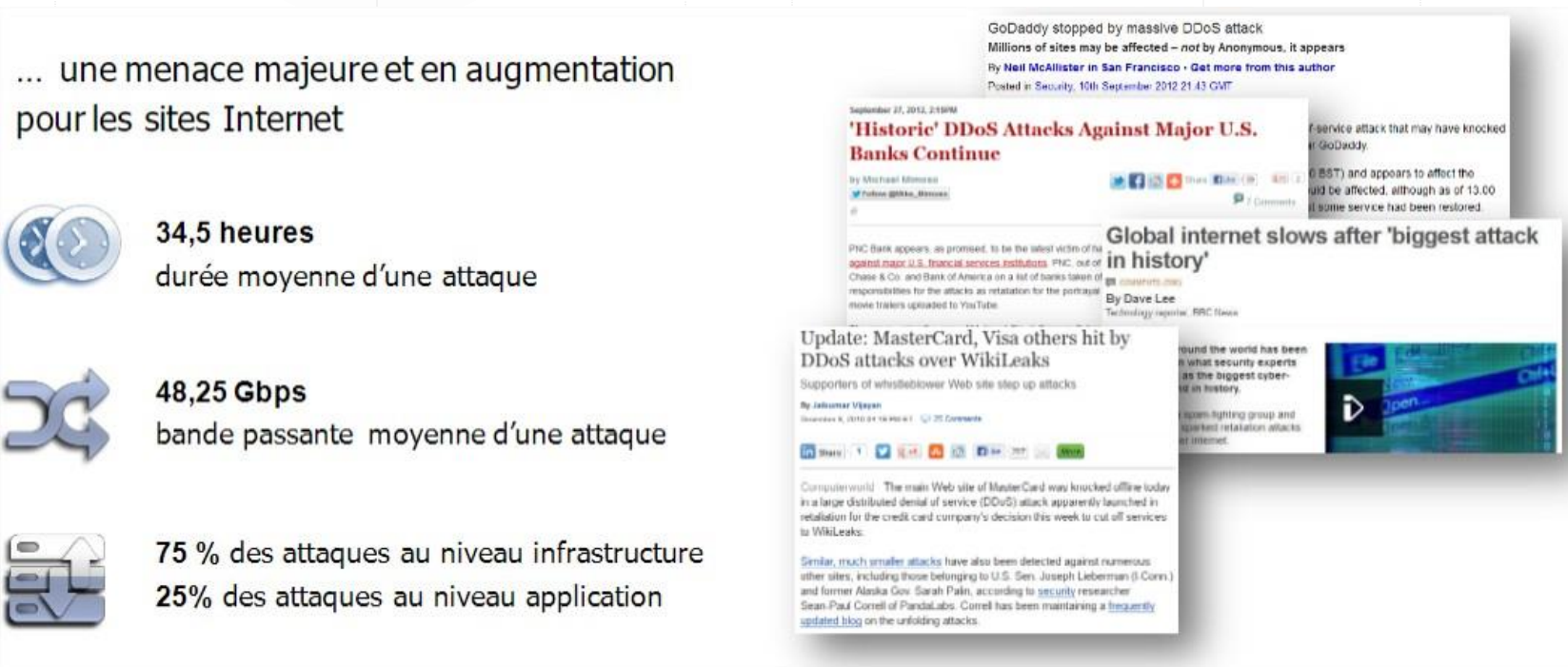
... avec comme conséquences potentielles ...

- Installation d'un « **cheval de Troie** » pour accéder au poste de travail à distance
- **Récupération de données** ciblées : cartes bancaires, identifiants/mots de passe...
- **Surveillance à distance** des activités : capture des écrans, des échanges, du son ou de la vidéo !
- **Destruction des données** des postes de travail
- **Chiffrement des données** pour une demande de rançon
- ...

4. Panorama de quelques menaces

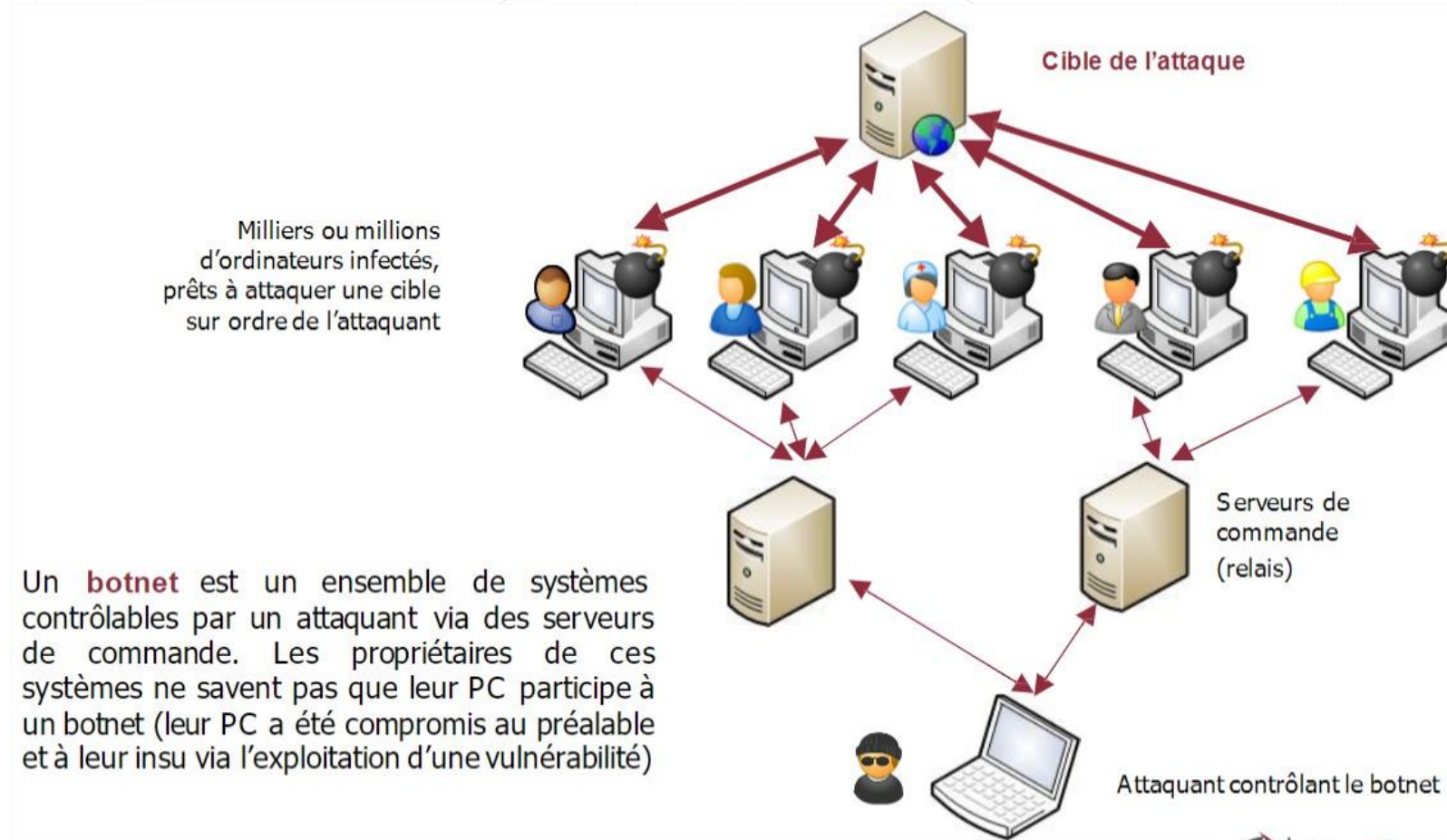
g. Déni de service distribué(DDoS)

Le **déni de service distribué(DDoS)** constitue une «**attaque ciblée**» qui consiste à saturer un site Web de requêtes pour le mettre «hors-service» à l'aide de «**botnets**», réseaux d'ordinateurs infectés et contrôlés par les attaquants



4. Panorama de quelques menaces

h. Illustration d'un réseau de botnets



Initiation à la cyber sécurité

Merci de votre attention