مكلية العلوم القانونية والإقتصادية والإجتماعية
FACULTÉ DES SCIENCES JURIDIQUES, ÉCONOMIQUES ET SOCIALES
ⵜⴰⵙⴷⴰⵡⵜ ⵏ ⵜⵣⵔⴼⵜ ⴰⵏⴰⵡⴰⵏ ⴷ ⵜⵙⴰⵡⴰⵍⵜ ⵜⵉⵎⵓⵔⴰⵏⵉⵢⵜ ⵜⵉⵏⵙⵜⵉⵜⵓⵜ ⵏ ⵜⵣⵔⴼⵜ ⵜⵉⵏⵙⵜⵉⵜⵓⵜ

MI@EG
FSJES - UMP - OUJDA

Sécurité Informatique des organisations

Année universitaire 2019/2020

Plan

- Introduction
- Définition de la SI
- Éléments à sécuriser
- Objectifs de SI
- Adversaires
- Faire confiance
- Moyens de protection
- La politique de SI
- Conclusion

Introduction

Notre objectif est d'identifier les attaques qui rendent l'entreprise vulnérable : menaces ***externes*** (Internet) ou ***internes***, ***logiciels malveillants*** et ***attaques*** affectant le ***système d'information***. Nous allons détailler les solutions efficaces à mettre en œuvre en rapport avec la criticité des informations, le contexte de l'entreprise et sa taille.

En effet, différentes technologies existent tant sur la partie système que réseau et demandent à être gérées à l'aide de pratiques simples et d'un minimum de bon sens pour garantir l'***intégrité***, la ***confidentialité***, la ***disponibilité*** des données et des applications.

La sensibilisation à tous ces aspects de la sécurité aidera à mieux maîtriser les outils dont-on dispose notamment pour la gestion des comptes d'accès aux serveurs et aux postes de travail.

Définition de SI (1)

- La sécurité informatique recouvre l'ensemble des techniques informatiques permettant de réduire au maximum les chances de fuites et/ou de modification de données ou de détérioration des Sys. d'Info.
- Elle consiste à un très grand nombre d'approches, de technologies, d'architectures permettant d'atteindre un certain niveau de protection.

Définition de SI (2)

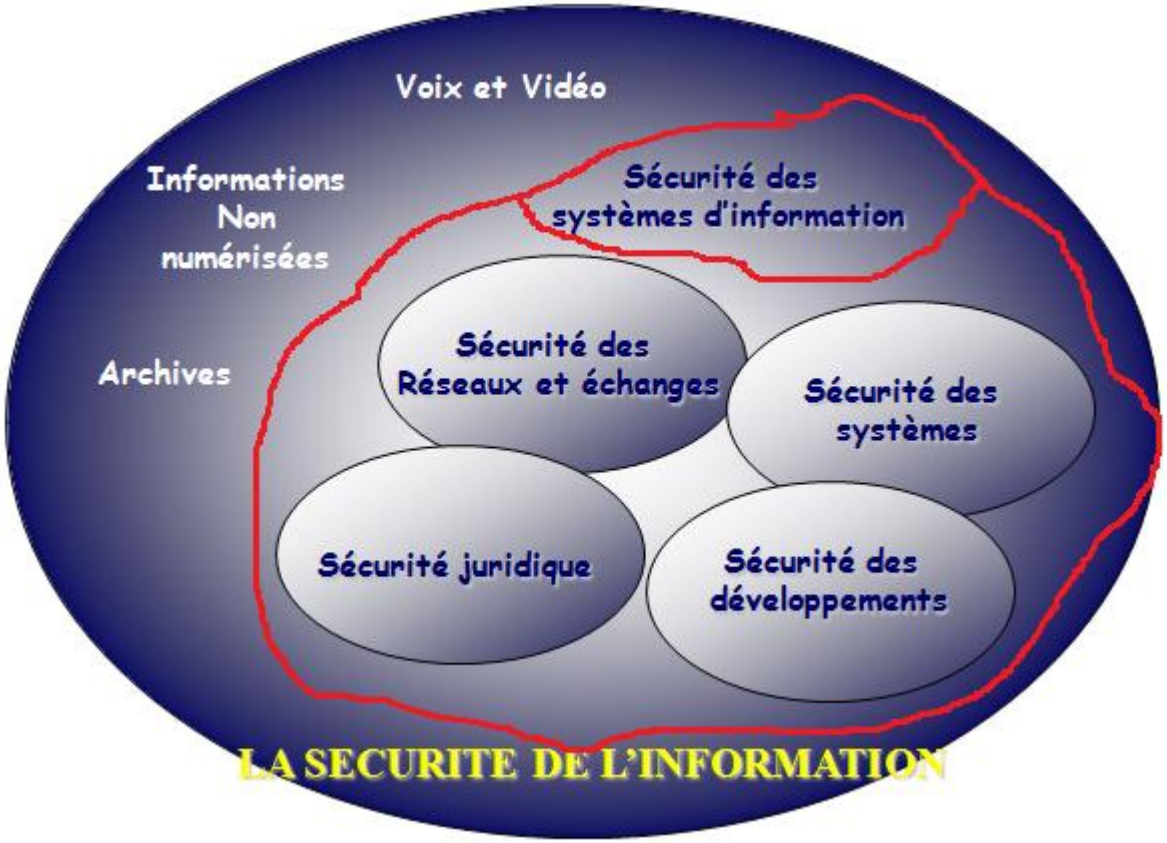
- "Sécuriser" consiste à utiliser une ou plusieurs techniques dans le but d'élever le niveau de sécurité d'un système ou d'une architecture.

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesure}}$$

  - La menace représente le type d'action susceptible de nuire dans l'absolu.
  - La vulnérabilité représente le niveau d'exposition face à la menace dans un contexte particulier.
  - Enfin la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

Eléments à sécuriser (1)

- L'« Information » au sens large.



Quelle que soit la forme prise par l'information ou quels que soient les moyens par lesquels elle est transmise ou stockée, il faut qu'elle soit toujours protégée de manière appropriée.

Seulement 40 à 50% des informations nécessaires pour faire fonctionner une entreprise sont enregistrées sur des supports électroniques

Eléments à sécuriser (2)

- Le triptyque DIC :
  - Disponibilité
    - Garantir que les utilisateurs habilités ont accès à l'information et aux ressources associées au moment voulu (pas d'accès non autorisé)
  - Intégrité
    - Sauvegarder l'exactitude et la fidélité de l'information et des méthodes de traitement des données (pas de modification non autorisée).
  - Confidentialité
    - Garantir que seules les personnes habilitées qui peuvent accéder à l'information (pas de divulgation non autorisée).

Eléments à sécuriser (3)

- Les actifs.
  - Les actifs sont caractérisés par leur type et surtout par leur valeur.

Actifs d'informations

Fichiers de données, bases de données Procédures et manuels utilisateurs, archives.

Actifs physiques

Serveurs informatiques, PC, portables, Matériels réseaux, unités de climatisation.

Actifs applicatifs

Progiciels, logiciels spécifiques, Systèmes d'exploitation, outils de développement, utilitaires.

Actifs liés à la fourniture de services

Services généraux (alimentation Électrique, climatisation, etc…)…

Objectifs de SI (1)

- L'information est une ressource stratégique, une matière première, elle est un atout pour celui qui la possède et donc attise souvent les convoitises.
- Les Sys. d'Info. facilitent l'accès à l'information
  - Ils gèrent de grandes quantités d'information et peuvent les rendre accessibles depuis n'importe quel point du globe.
- La destruction d'un Sys. d'Info. peut permettre d'anéantir une entité de manière anonyme.
- La loi, la réglementation et l'éthique seront toujours en retard sur la technique.
- Les individus se comportent rarement comme on l'attend.
  - Le comportement d'un individu confronté à des situations inhabituelles et critiques est imprévisible.

Objectifs de SI (2)

- Les conséquence à retenir
  - Vol d'informations et du savoir faire
    - Dans un contexte de haute technologie notamment
  - Atteinte à l'image de marque
    - NASA, e-bay, Wanadoo, RSA, …
  - Indisponibilité du service
    - e-business, …
  - Perte de temps et de moyen humains
    - Remise en service, recherche des dégradations
      - Tache TRES difficile, peut nécessiter des moyens énormes
  - Pertes financières !
    - Modification des comptes bancaires …
    - Perte d'exploitation
    - Erreurs de traitement

Adversaires

- Les menaces
- Les différents types de pirates
- Les différentes arnaques et attaques
- Les accidents et inconsciences

La menace - Définitions

- *« Violation potentielle de la sécurité » - ISO-7498-2*
  - Menace accidentelle
    - Menace d'un dommage non intentionnel envers le Sys. d'Info.
      - Catastrophe naturelle, erreur d'exploitation, pannes
  - Menace intentionnelle ou délibérée
    - Par opposition à la précédente, elle est le fait d'un acte délibéré
    - Menace active
      - Menace de modification non autorisée et délibérée de l'état du système d'info.
        - » Dommage ou altération du Sys. d'Info.
    - Menace Passive
      - Menace de divulgation non autorisée des informations, sans que l'état du Sys. d'Info. soit modifié.
        - » Écoutes, lecture de fichiers, …
    - Menace Physique
      - Menace l'existence ou l'état physique du Sys. d'Info.
        - » Sabotage, incendie volontaire, vol, …

Catégories de menaces intentionnelles

- L'espionnage
  - Obtention d'informations
- Le vol
  - Obtention d'informations ou de ressources
- La perturbation
  - Affaiblir le Sys. d'Info.
- Le sabotage
  - Mise hors service du Sys. d'Info.
- Le chantage
  - Gain financier, menace de sabotage, …
- La fraude physique (récupération de bandes, listings, …)
  - Obtention d'informations
- Les accès illégitimes (usurpation d'identité)
  - Obtention d'informations

Origines / Attaquants (1)

- Accidents
  - Type de menace
    - Menaces accidentelles (cf. définition)
  - Type d'attaquants
    - La nature !
      - Incendies, Foudre, Inondations, etc…
    - Les fournisseurs
      - Fournisseurs de connectivité, Fournisseurs de matériels et de logiciels, …
    - Agresseurs internes (La majorité des cas)
      - Inconsciences et accidents (A ne pas négliger !)
        - » Provoqués par l'inattention ou le manque de formation des administrateurs ou des utilisateurs

Origines / Attaquants (2)

- Menaces à caractère stratégiques
  - Type de menace
    - Menace intentionnelle active, passive et physique
    - Pour un état
      - Le secret défense et la sûreté de l'état
      - Le patrimoine scientifique, technique, économique, diplomatique
      - La disponibilité des Sys. d'Info. et le fonctionnement des institutions
    - Pour l'entreprise
      - Informations concernant ses objectifs et son fonctionnement
      - Les clients, procédés de fabrication, recherche et développement
  - Catégories de menace
    - Espionnage, vol, perturbation, sabotage, fraude physique, accès illégitimes …
  - Type d'attaquants
    - Espions
      - Particuliers (rare), Entreprises, Gouvernements
    - Terroristes

Origines / Attaquants (3)

- Menace à caractère idéologique
  - Type de menace
    - Menace intentionnelle active, passive et physique
    - Le combat pour les idées est incessant et peut être le moteur d'actes les plus extrêmes
      - Idéologie politique, raciale, religieuse, économique, …
  - Catégorie de menace
    - Espionnage, vol, perturbation, sabotage, chantage, fraude physique, accès illégitimes, …
  - Type d'attaquants
    - Militants
    - Vandales
    - Terroristes

Origines / Attaquants (4)

- Menace à caractère terroriste
  - Type de menace
    - Menace intentionnelle active, passive et physique
    - Actions concourant à déstabiliser l'ordre établi
      - A caractère violant : destruction
      - A caractère insidieux : désinformation, détournements
  - Catégorie de menace
    - Espionnage, vol, perturbation, sabotage, chantage, fraude physique, accès illégitimes, …
  - Type d'attaquants
    - Terroristes

Origines / Attaquants (5)

- Menace à caractère cupide
  - Type de menace
    - Menace intentionnelle active, passive et physique
    - But d'attaquant
      - Financier, technologique, …
    - Pertes pour la victime
      - Entraînant un gain pour l'agresseur : parts de marché, déstabilisation du concurrent, …
  - Catégorie de menace
    - Espionnage, vol, perturbation, sabotage, chantage, fraude physique, accès illégitimes, …
  - Type d'attaquant
    - Espions (concurrent)
    - Crime Organisé
    - Intervenants
      - Ont souvent accès à des informations sensibles, et conservent souvent des fichiers de configuration, …

Origines / Attaquants (6)

- Menace à caractère ludique
  - Type de menace
    - Menace intentionnelle active
    - Désir de s'amuser ou d'apprendre
      - C'est le travail technique qui est mis en avant
  - Catégorie de menace
    - Vol, perturbation, sabotage, accès illégitimes, …
  - Type d'attaquant
    - « Joyriders »
    - Vandales
    - Collectionneurs

Généralement appelés

Hackers ou Crackers

Origines / Attaquants (7)

- Menace à caractère vengeur
  - Type de menace
    - Menace intentionnelle active, passive et physique
    - Également un moteur d'actes extrêmes
      - Souvent l'expression d'un employé brimé ou licencié qui peut posséder une très bonne connaissance du Sys. d'Info.
  - Catégorie de menace
    - Vol, perturbation, sabotage, accès illégitimes, …
  - Type d'attaquant
    - Personnes extérieures en désaccord avec l'organisation
      - Peur être un client, un fournisseur, un intervenant, …
    - Les employés malveillants ou aigris
      - Ont souvent une bonne connaissance de l'organisation
      - Utilisateurs dépassant leurs prérogatives
      - Administrateurs, informaticiens, …

Origines / Attaquants (8)

- La liste des attaques est non exhaustive.
- La menace peut être composite
  - Plusieurs motivations (origines)
    - Cupide + Ludique, Idéologique + Terroriste, …
  - Plusieurs profils de pirate
    - Employé malveillant + Espion, …
- Les ***Hackers*** [*white hats (*alertent le propriétaire sur les failles de sécurité de son système afin de l'aider à le sécuriser) *& black hats (*pirates malfaisants)], les ***Crackers*** (genre de hackers spécialisés dans le contournement des protections anticopies des logiciels) et les ***Phreakers*** *(*inventent des systèmes qui permettent de téléphoner gratuitement ou de modifier le contenu des téléphones mobiles) monopolisent l'attention mais ne sont en réalité qu'une composante de la problématique de sécurité !

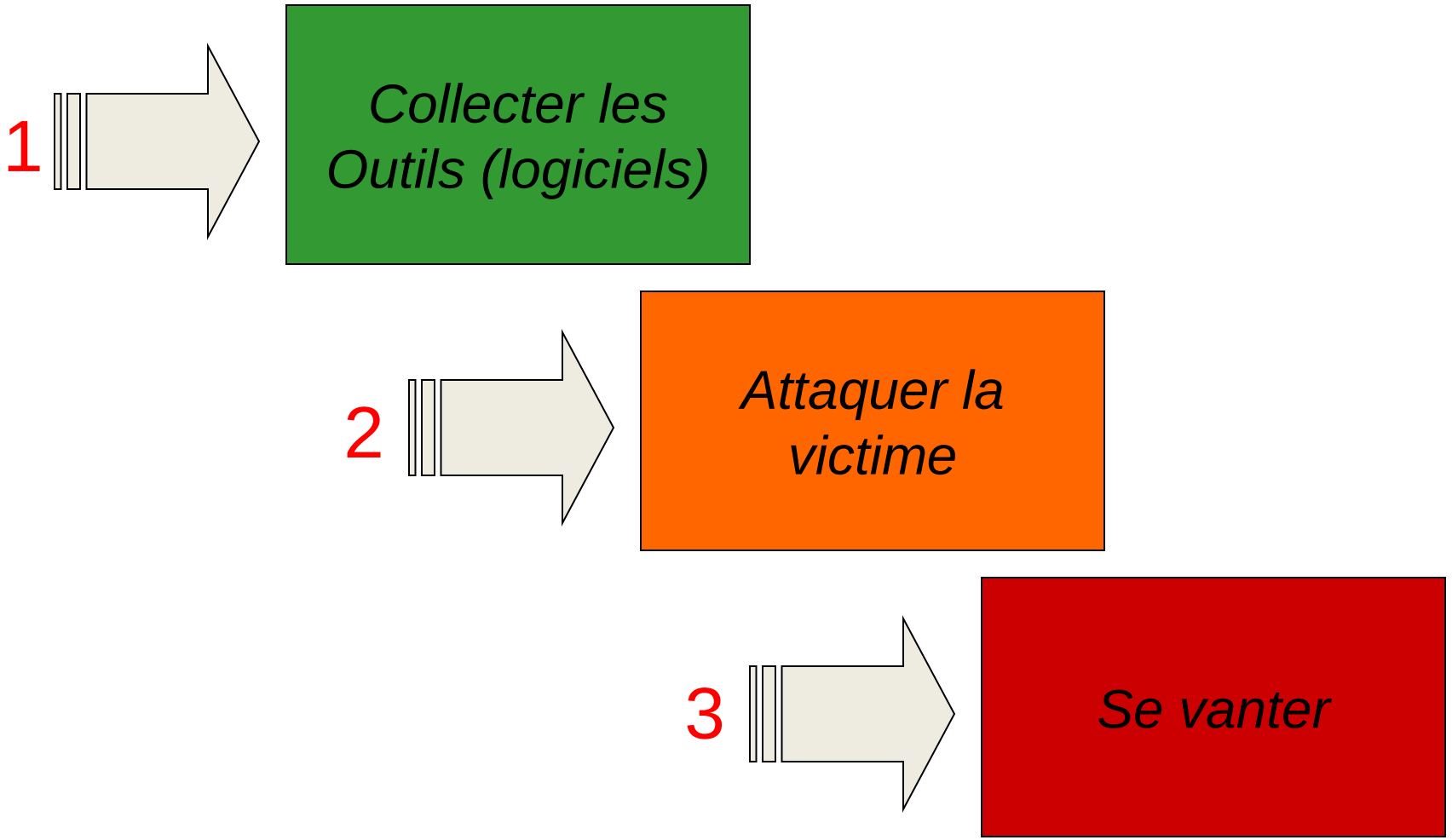
Adversaires - Critères

- Comment caractériser les agresseurs ?
  - Leurs compétences techniques
  - Le temps qu'ils sont prêts à passer pour réussir
  - Leurs motivations
  - Leurs moyens
  - Leurs connaissances préalables de la cible

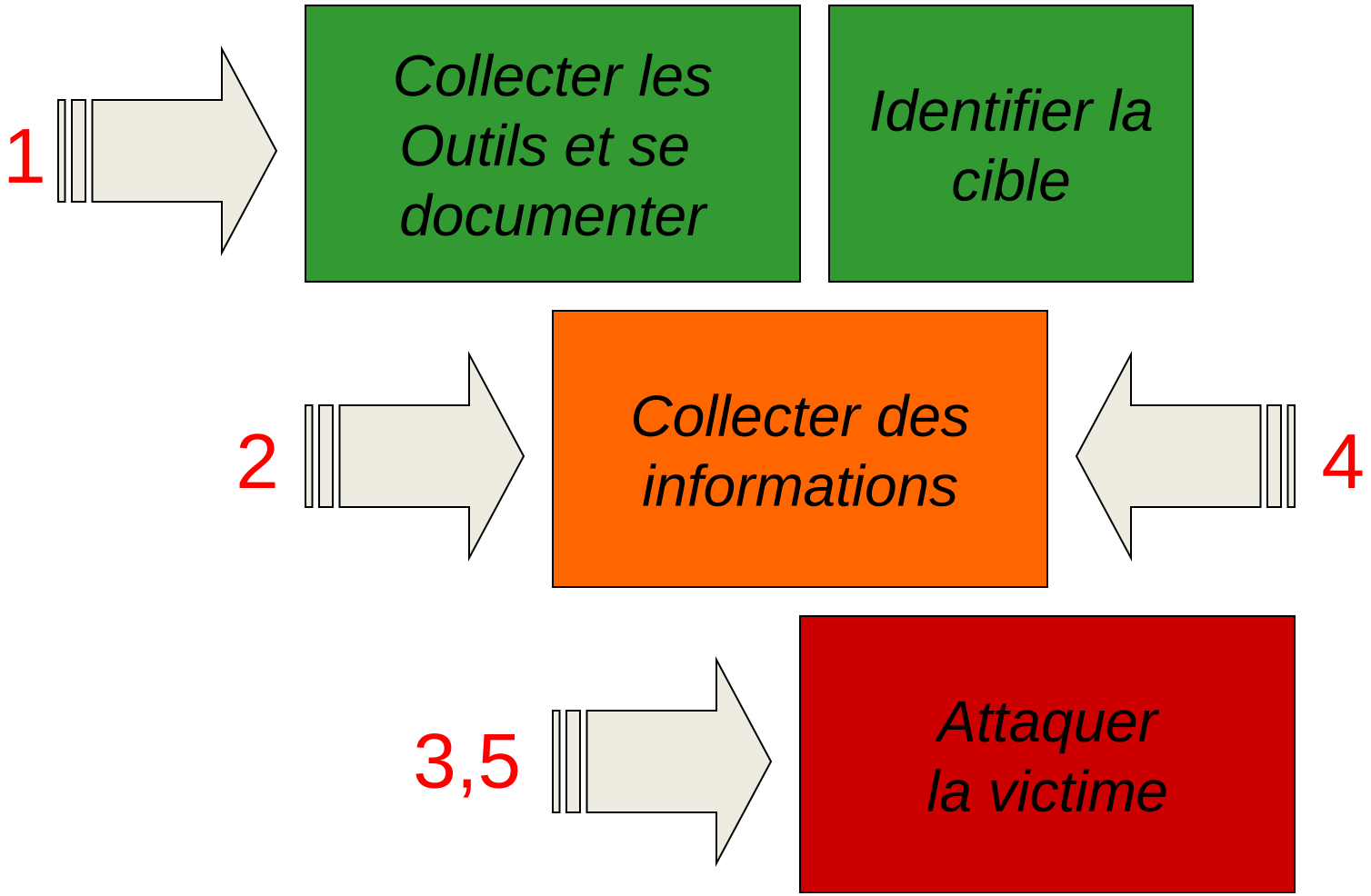
Classement

	Compétence	Temps	Motivation
Un hacker / étudiant externe pour le plaisir	Forte	Fort	Moyenne
Un concurrent	Forte	Faible	Forte
Un escroc (enjeu financier)	Moyenne	Moyen	Moyenne
Un opportuniste	Faible	Faible	Faible
Un membre de société de service	Forte	Faible	Faible
Un ancien membre du personnel	Moyenne	Faible	Moyenne
Un membre du personnel	Moyenne	Faible	Faible
Un stagiaire	Forte	Moyen	Faible

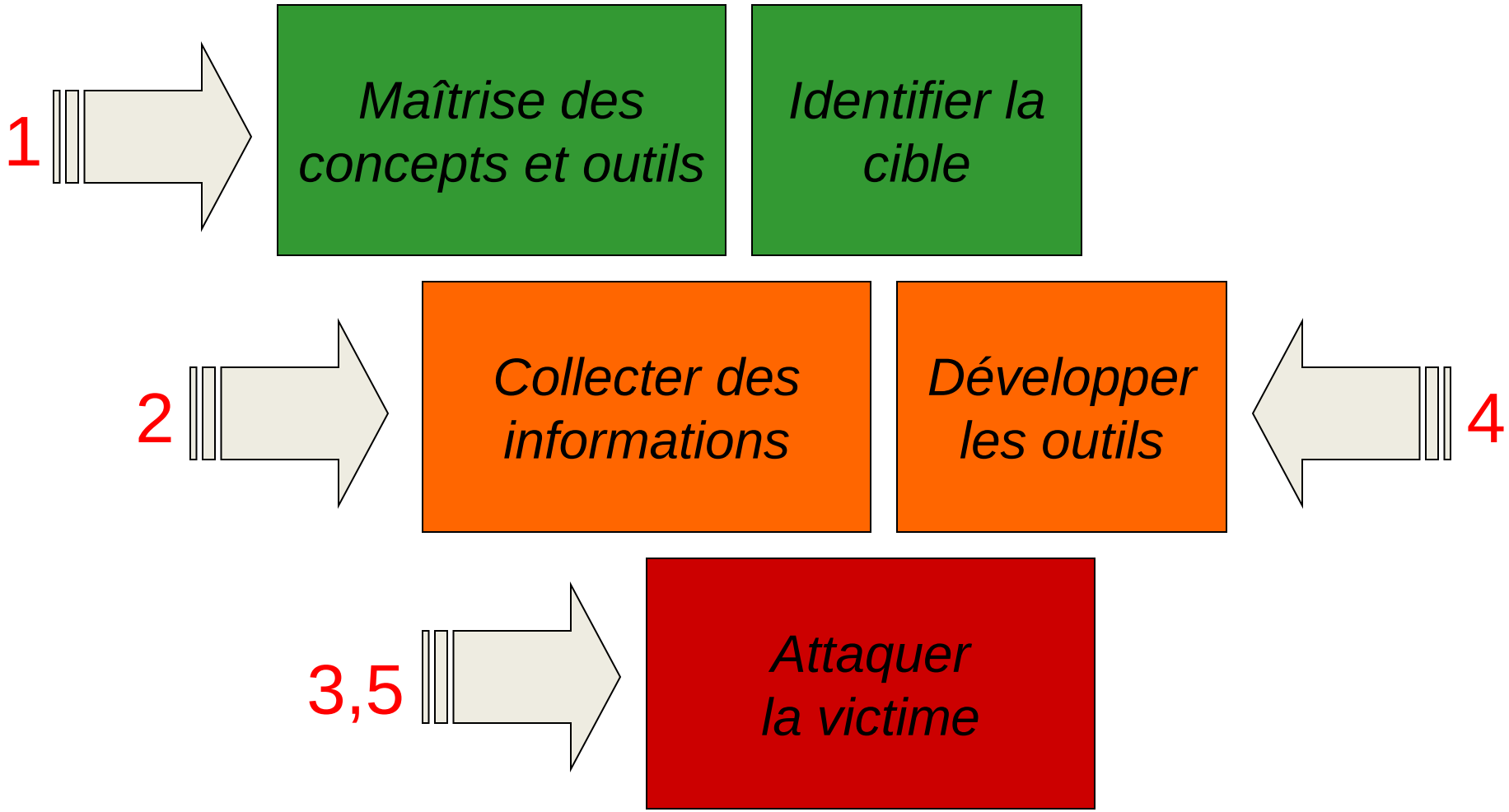
Démarche basique (Cracker)



Démarche intermédiaire



Démarche expert (Hacker)



Attaques != Vulnérabilité

- Attaque
  - Action de malveillance consistant à tenter de contourner les fonctions de sécurité d'un Sys. d'Info.
- Vulnérabilité
  - Faiblesse ou faille dans les procédures de sécurité, les contrôles administratifs, les contrôles internes d'un système, qui pourrait être exploitée pour obtenir un accès non autorisé au Sys. d'Info., à un de ses services, à des informations ou à la connaissance de leur existence et de permettre de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité du Sys. d'Info. et de ses informations.

Attaques != Vulnérabilité

- Dans la conception
  - Matériel
  - Protocoles
  - Architectures (Sys. Info., Réseau, …)
  - Logiciels (OS, Applications, …)
- Dans l'implémentation
  - Matériel
  - Protocoles
  - Architectures (Sys. Info., réseau …)
  - Logiciels (OS, Applications, …)
- Configuration, exploitation
  - Équipement (Routeurs, Firewalls, Serveur, …)
  - Logiciel (OS, Applications, …)

Attaques (1)

- Intrusions
- Vandalisme
- Denis de service (DOS)
- Vol d'informations
- Escroqueries

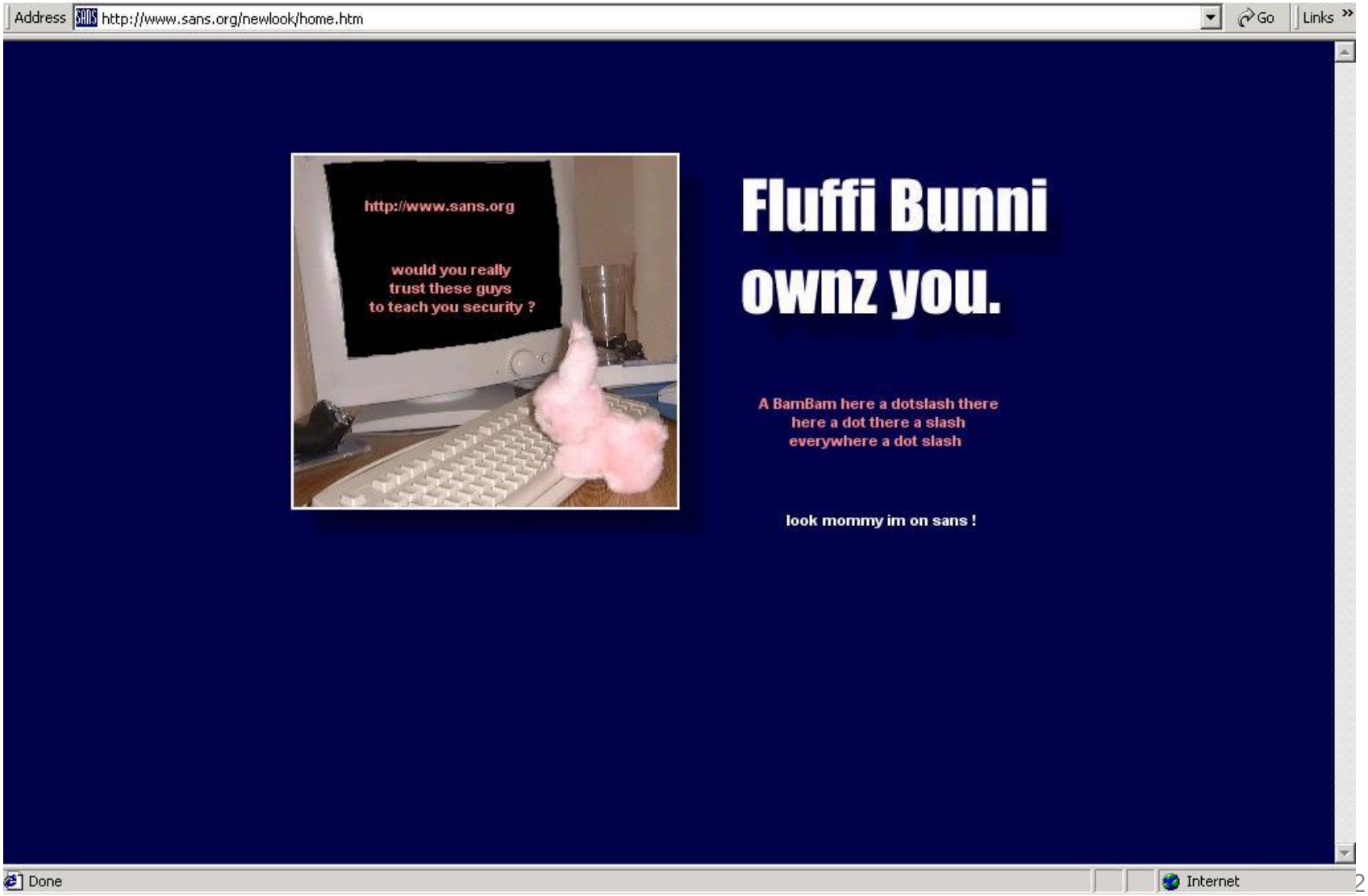
Attaques (2)

- ***Intrusions***
  - Recherche de mots de passe
    - Dictionnaire (en utilisant les algorithmes de chiffrement)
    - Écoute du réseau (en utilisant la topologie logique Token Ring)
    - « Brute force » : Cette technique consiste à deviner un mot de passe en testant, de manière automatisée, toutes les solutions possibles jusqu'à tomber sur la bonne.
  - Le « Spoofing »
  - Les sniffers et scanners
  - Les exploits

Attaques (3)

- ***Vandalisme***
  - Destruction de fichiers
  - Destruction de systèmes
  - Défiguration de site Web

Attaques (3)


Address
http://www.sans.org/newlook/home.htm
Go
Links
http://www.sans.org
would you really
trust these guys
to teach you security ?
Fluffi Bunni
ownz you.
A BamBam here a dotslash there
here a dot there a slash
everywhere a dot slash
look mommy im on sans !
Done
Internet

Attaques (4)

- ***Denis de service (DOS)***
  - Bombes logiques (virus)
  - Le « flood »
    - TCP-SYN Flooding : Elle s'applique dans le cadre du protocole TCP et consiste à envoyer une succession de requêtes synchronisées vers la cible.
  - Le « Nuke »: Plantage de Windows dus à des utilisateurs peu intelligents (qui connaissent votre adresse IP)
  - Le « spamming »
- Denis de service distribué (DDOS)
  - Amplification des DOS

Attaques (5)

- ***Vol d'information***
  - Suite à une intrusion
  - Interception
  - Écoute
  - Cryptanalyse

Les principales escroqueries (1)

- ***L'ingénierie sociale***
  - Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs.
  - Elle consiste à exploiter non pas une faille informatique mais la «faille humaine» en dupant les internautes par le biais d'un faux site, d'un courrier électronique, d'un appel téléphonique semblant provenir d'une entreprise de confiance, d'un courrier traditionnel ou contact direct.

Les principales escroqueries (2)

- ***Le scam***
  - Un internaute vous demande de servir d'intermédiaire pour une transaction financière importante, en vous promettant un bon pourcentage de la somme, et pour amorcer la transaction, il vous faut donner de l'argent..

Les principales escroqueries (3)

- ***Le phreaking***
  - Contraction des mots anglais phone (téléphone) et freak (monstre) désignant le piratage de lignes téléphoniques
    - Technique frauduleuse permettant l'utilisation gratuite de ressources téléphoniques depuis l'extérieur.
    - Piratage du téléphone d'un abonné, accessible depuis l'extérieur, dans le but de prendre le contrôle de son installation et activer des fonctions de renvoi d'appels vers l'extérieur.

Les principales escroqueries (4)

- ***L'hameçonnage (Le phishing)***
  - Contraction des mots anglais «fishing» et «phreaking»
    - Technique d'«ingénierie sociale» qui consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration...) afin de lui soutirer des données personnelles (mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte nationale d'identité, date de naissance…)

Les principales escroqueries (5)

- ***Le canular (Hoax)***
  - il s'agit d'une information erronée ou invérifiable qui profite de la puissance d'Internet pour se propager à grande échelle. Ça peut être un courriel, un message publié sur des forums ou les réseaux sociaux et dont les contenus cherchent à créer l'inquiétude, l'indignation ou au contraire l'approbation.
  - Les conséquences:
    - L'engorgement des réseaux et des serveurs de messagerie,
    - Une désinformation, c'est-à-dire faire admettre à de nombreuses personnes de faux concepts ou véhiculer de fausses rumeurs,
    - La perte du temps, tant pour ceux qui lisent l'information, que pour ceux qui la relayent ;
    - La dégradation de l'image d'une personne ou bien d'une entreprise,
    - L'incrédulité : à force de recevoir des fausses alertes, les usagers du réseau risquent de ne plus croire aux vraies (comme exemple le débattre inverse d'une religion).

Les virus (1)

- Le virus informatique (Malware) est un programme situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé.
- Différents types:
  - Les vers
  - Les troyens (Les chevaux de Troie)
  - Les bombes
  - Les spywares (Les espiogiciels)

Les virus (2)

- ***Les vers***
  - Un ver informatique se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il est conçu pour se copier d'un ordinateur à un autre automatiquement.
  - Un ver se propage généralement sans action de l'utilisateur et distribue des copies complètes de lui-même de réseaux en réseaux. Il peut consommer de la mémoire ou de la bande passante réseau, ce qui peut entraîner une panne d'ordinateur.
  - Comme les vers n'ont pas besoin d'un programme ou d'un fichier "support" pour se répandre, ils peuvent ouvrir un tunnel dans votre système et permettre à une autre personne de contrôler votre ordinateur à distance.

Les virus (3)

- ***Les chevaux de Troie (Les troyens)***
  - Programme (en anglais trojan horse) caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (en anglais backdoor).
  - Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur.
    - Vol des mots de passe,
    - Copie des données,
    - Exécution d’action nuisible.

Les virus (4)

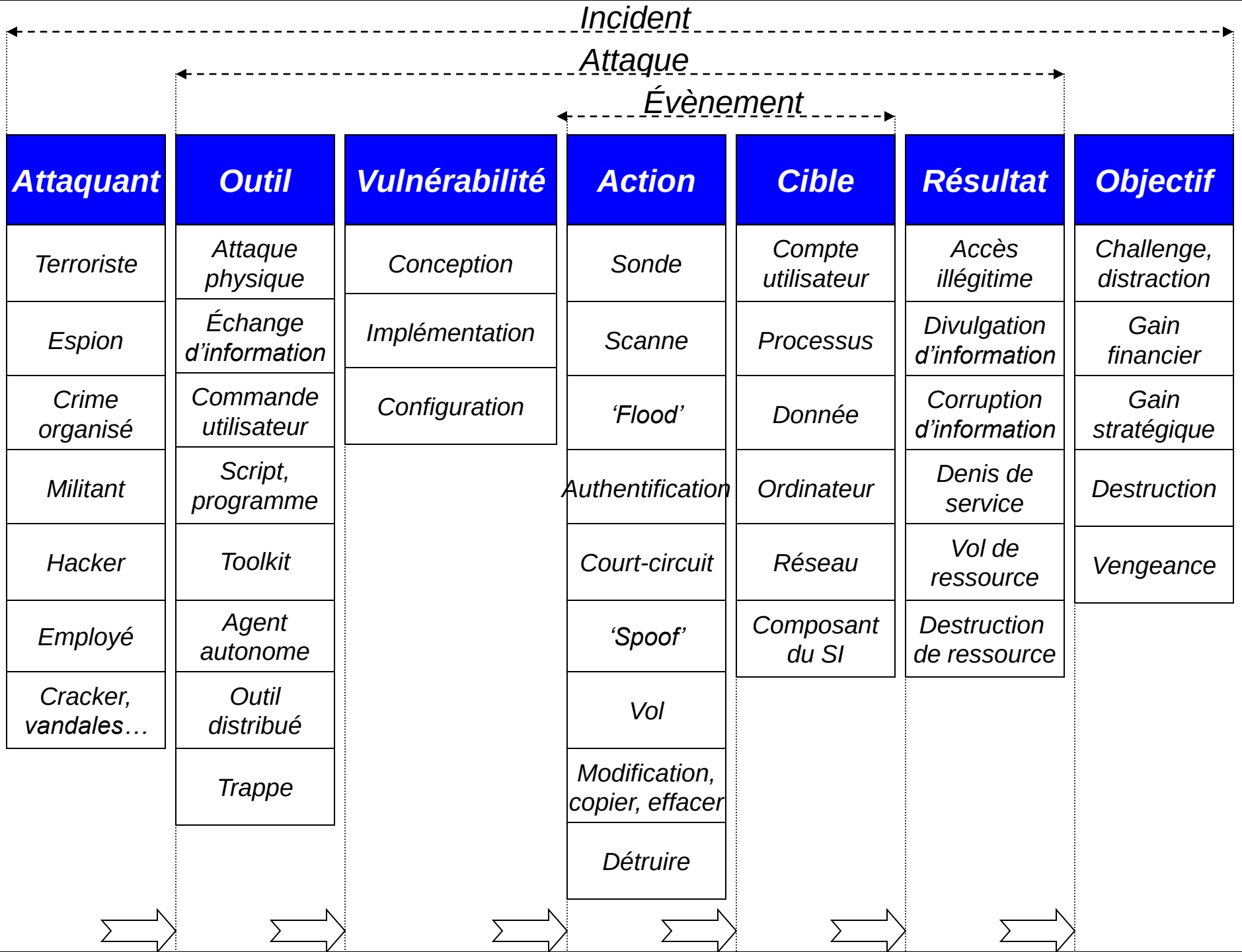
- ***Les bombes logiques***
  - Dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système.
  - Généralement elles s’utilisent dans le but de créer un déni de service.
    - Exemple la bombe logique Tchernobyl s'est activée le 26 avril 1999.

Les virus (5)

- ***Les spywares ou espiogiciels***
  - Contraction des mots anglais *spy* «espion» et *software* «logiciel», le terme «spyware» désigne un logiciel espion qui collecte des données personnelles afin de les envoyer à un tiers.
  - Ce type de programme malveillant est la plupart du temps caché dans des logiciels gratuits mais il peut aussi se propager depuis une page Internet infectée. On en trouve notamment sur les sites Web proposant des contenus illégaux.
    - Keyloggers : Dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif ***d'espionnage***.

Taxinomie d'un incident

- Taxinomie (ou Taxonomie)
  - Classification d'éléments selon des taxons
- Taxon (biologie)
  - Unité formelle représentée par un groupe d'organismes, à chaque niveau de la classification.


Incident
Attaque
Évènement
Attaquant
Outil
Vulnérabilité
Action
Cible
Résultat
Objectif
Terroriste
Espion
Crime organisé
Militant
Hacker
Employé
Cracker, vandales…
Attaque physique
Échange d'information
Commande utilisateur
Script, programme
Toolkit
Agent autonome
Outil distribué
Trappe
Conception
Implémentation
Configuration
Sonde
Scanne
'Flood'
Authentification
Court-circuit
'Spoof'
Vol
Modification, copier, effacer
Détruire
Compte utilisateur
Processus
Donnée
Ordinateur
Réseau
Composant du SI
Accès illégitime
Divulgation d'information
Corruption d'information
Denis de service
Vol de ressource
Destruction de ressource
Challenge, distraction
Gain financier
Gain stratégique
Destruction
Vengeance

Faire confiance

- Personne !!
- Tout le monde n'est pas mal intentionné
  - Il existe des gens mal intentionnés
  - Il existe des gens bien intentionnés mais irresponsables (Microsoft, ebay,…)
- A qui fait-on confiance ?
  - Éditeurs
  - Partenaires
  - Intervenants (SSII, intégrateurs, consultants, …)
- S'assurer qu'ils sont aussi rigoureux que vous sur la sécurité !!

Moyens de protection

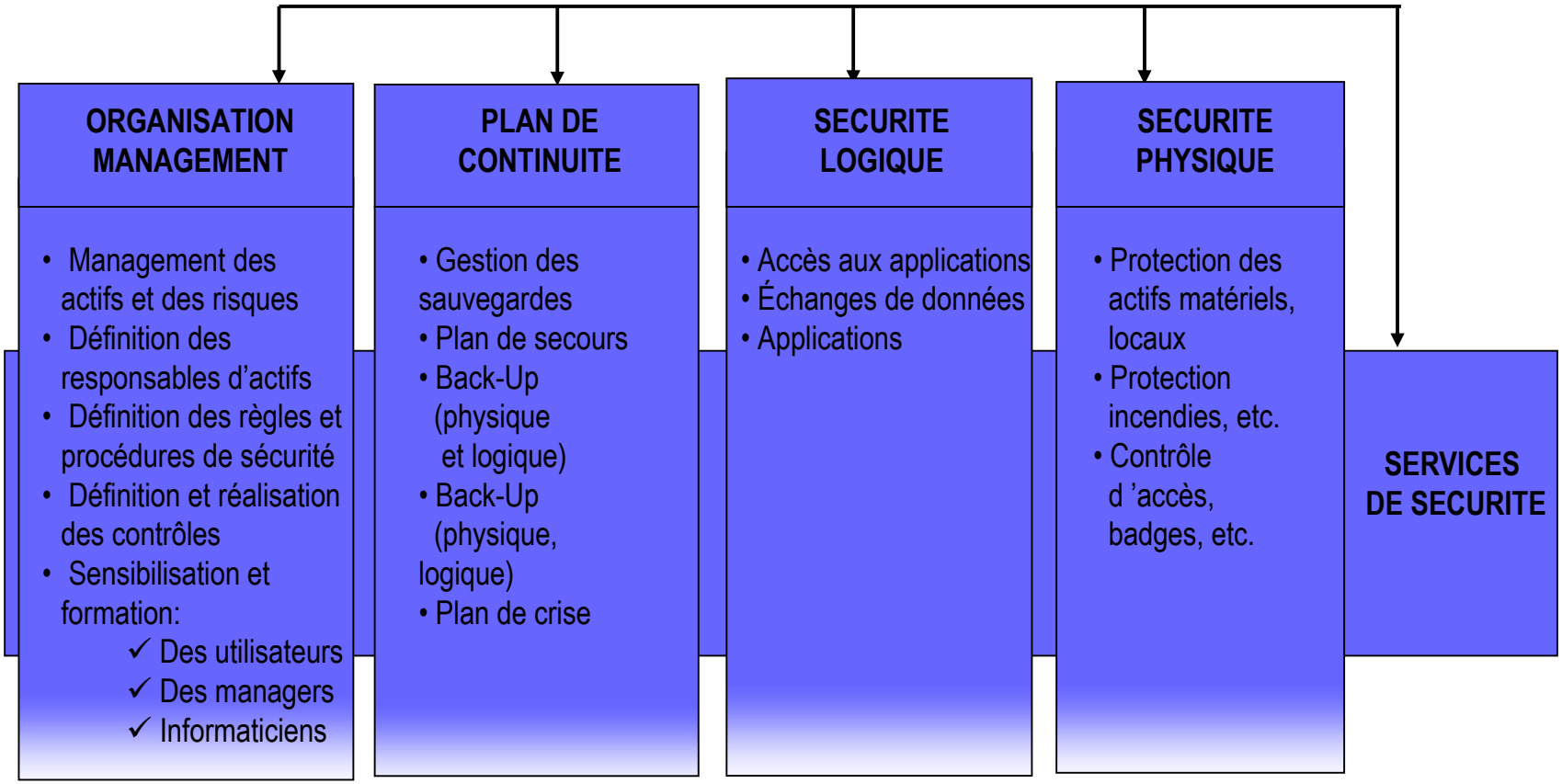
- Pas de sécurité totale!!
- Miser sur la discrétion,
- Sécurité des systèmes d'information,
- Sécurité du réseau informatique et téléphonique,
- Sensibiliser et former le personnel,
- Aucun modèle de sécurité ne peut résoudre tous les problèmes:
  - Définir une politique de sécurité au sein de votre organisation.
  - Définir une démarche de sécurité.

La politique de sécurité (1)

- C’est un dispositif global dont la mise en œuvre assure que l’information peut être partagée d’une façon qui garantit un niveau approprié de protection de cette information et des actifs liés.
- Toutes méthodes, techniques et outils utilisés pour protéger l’information contre un large éventail de menaces afin :
  - De garantir la continuité de l’activité de l’entreprise,
  - De réduire les dommages éventuels sur l’activité de l’entreprise,
  - De maximiser le retour au investissement sur les Systèmes d’Information.

La politique de sécurité (2)

- Les domaines.



Les mesures élaborées dans un plan de sécurité peuvent-être classées en deux familles :

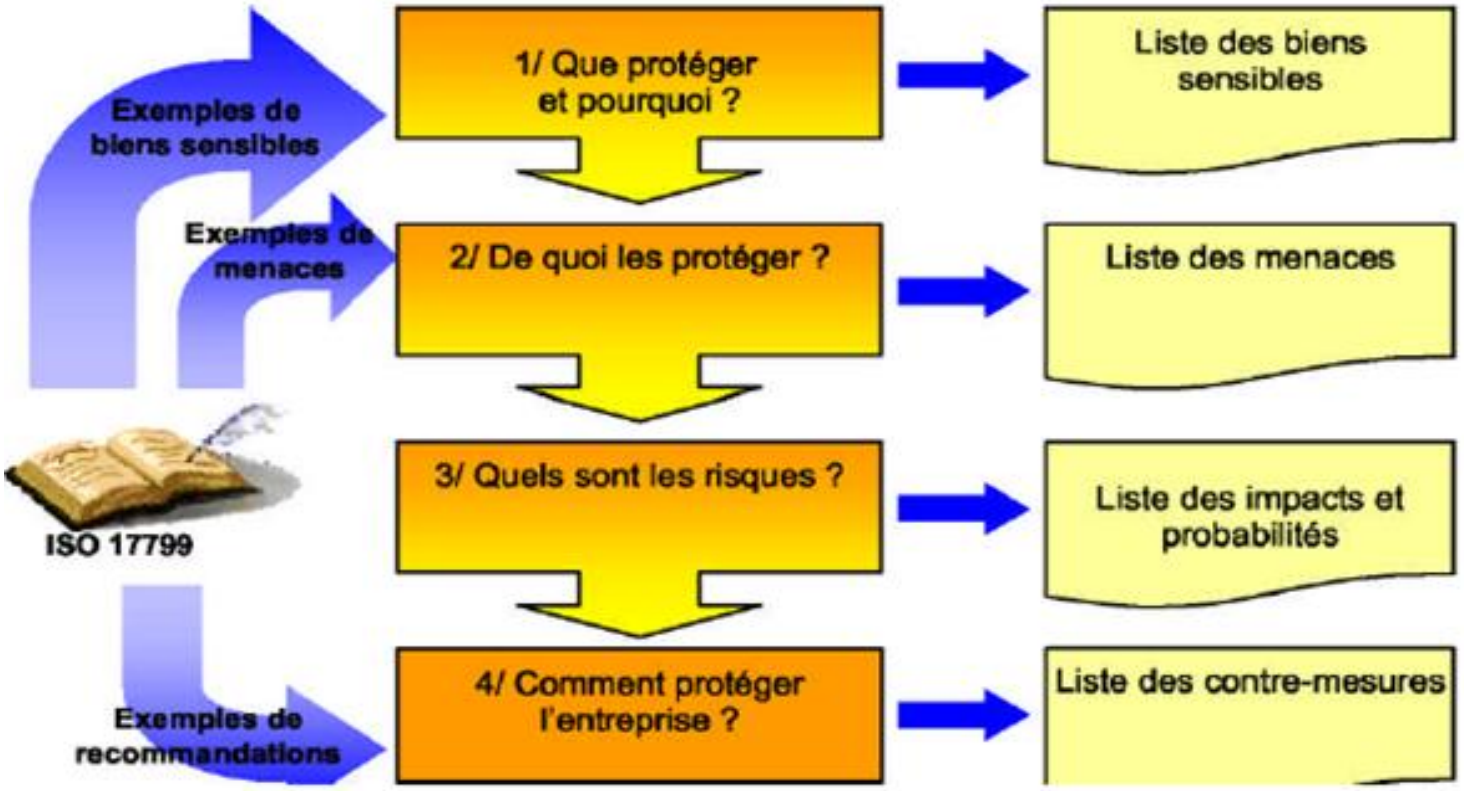
- avant sinistre : mesure de prévention

- après sinistre : détection, ralentissement, correction

REMARQUE

La politique de sécurité (3)

- La démarche type.



La politique de sécurité (4)

- Les différentes approches.

Approche française: CLUSIF

Analyse des enjeux et des risques

·Assez similaire à une démarche qualité,

· Plusieurs méthodologies disponibles: MEHARI, EBIOS,…

· **Avantages**: Développement de la culture du risque, implication du personnel, pertinence,

· **Inconvénients**: Coût (ressources humaines).

Approche anglo-saxonne

Approche par les bonnes pratiques

·Recueil de procédures, fiches, Contrôles,

· Le recueil le plus connu est ISO 17799,

· **Avantages**: Efficacité, exhaustivité,

· **Inconvénients**: Coût.

Approche SSU
(Solution de sécurité d'Urgence)

·Mise en oeuvre d'une batterie D'outils techniques,

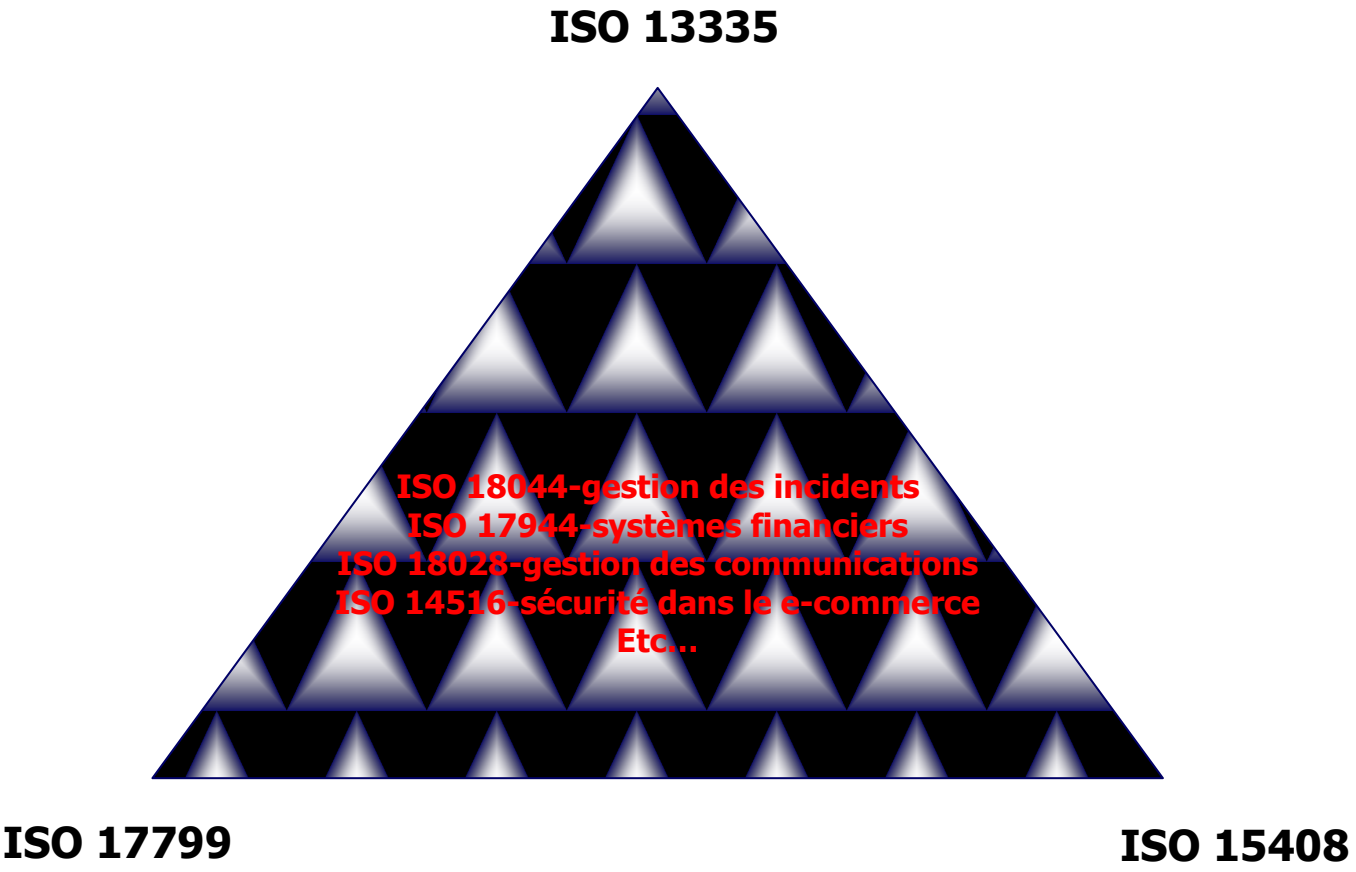
· Pare-feux, anti-virus, VPN, SSL, anti-SPAM, etc…

· **Avantages**: Délais de mise en oeuvre, investissement uniquement Matériel/logiciel,

· **Inconvénients**: Donne un faux Sentiment de sécurité.

La politique de sécurité (5)

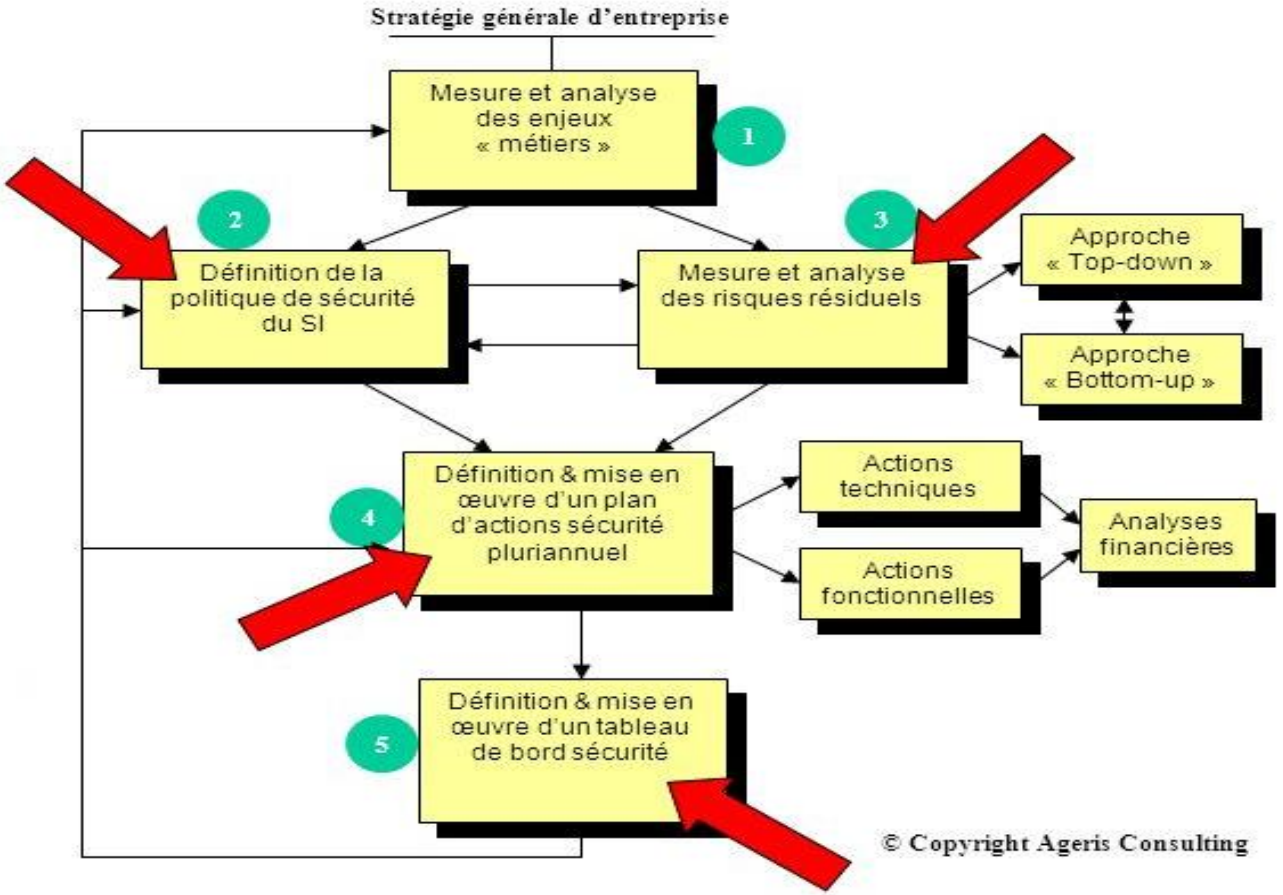
- Les normes ISO concernant la sécurité.



La politique de sécurité (6)

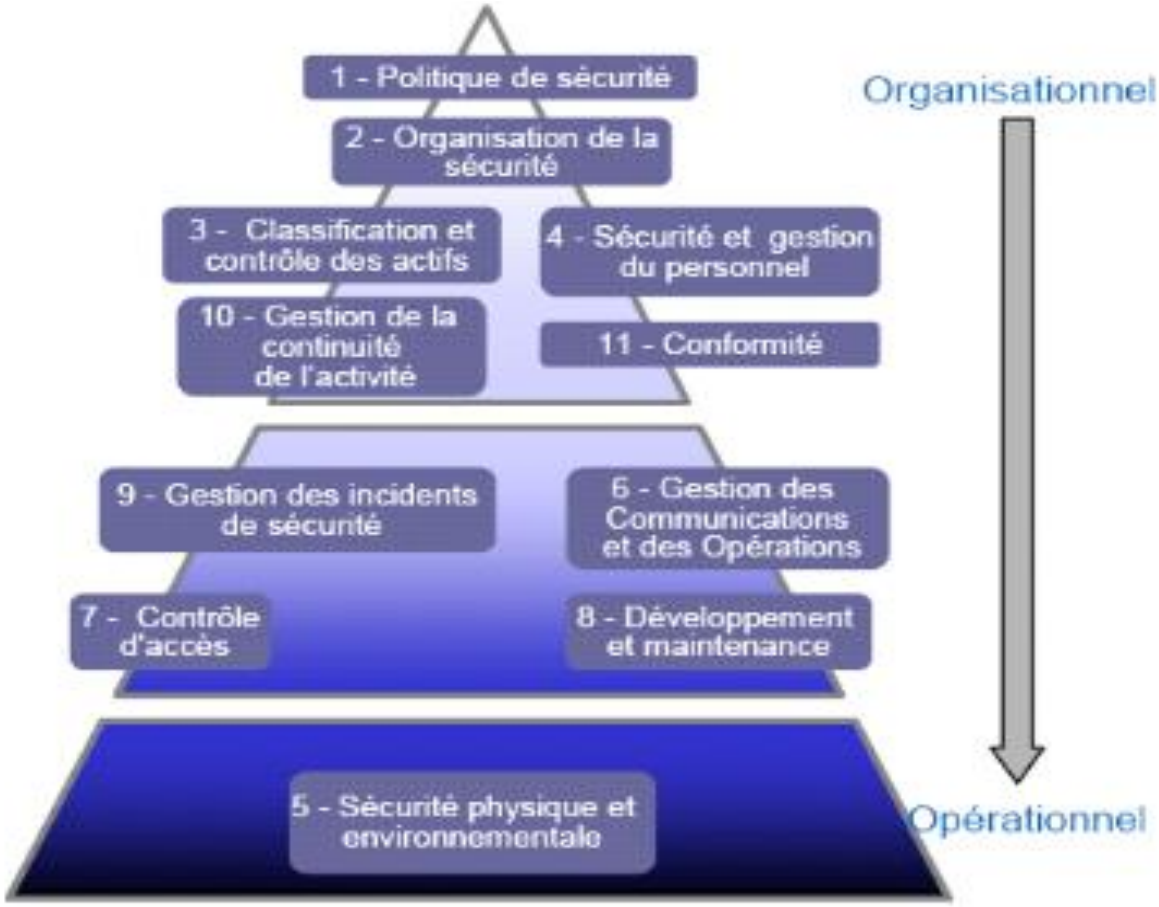
Synthèse de l'utilisation de la norme ISO 17799

La norme ISO 17799 est un bon outil pour la gouvernance des risques



La politique de sécurité (7)

- Les normes de sécurité de l'information actuelles



Les méthodes de sécurité

- Les plus connues sont MEHARI (Clusif), EBIOS (DCSSI) et MARION (Clusif).
  - Ces méthodes ont leurs propres référentiels qui ne couvrent pas toujours strictement le spectre de l'ISO 17799,
  - Il peut par conséquent être nécessaire de retravailler les bases de connaissance de ces méthodes pour obtenir une couverture complète de la sécurité de l'Information,
  - La commission du Clusif a corrélé la base de connaissance de MEHARI afin de couvrir l'ensemble des mesures de ISO 17799.

Système de Management de la Sécurité de l'Information (1)

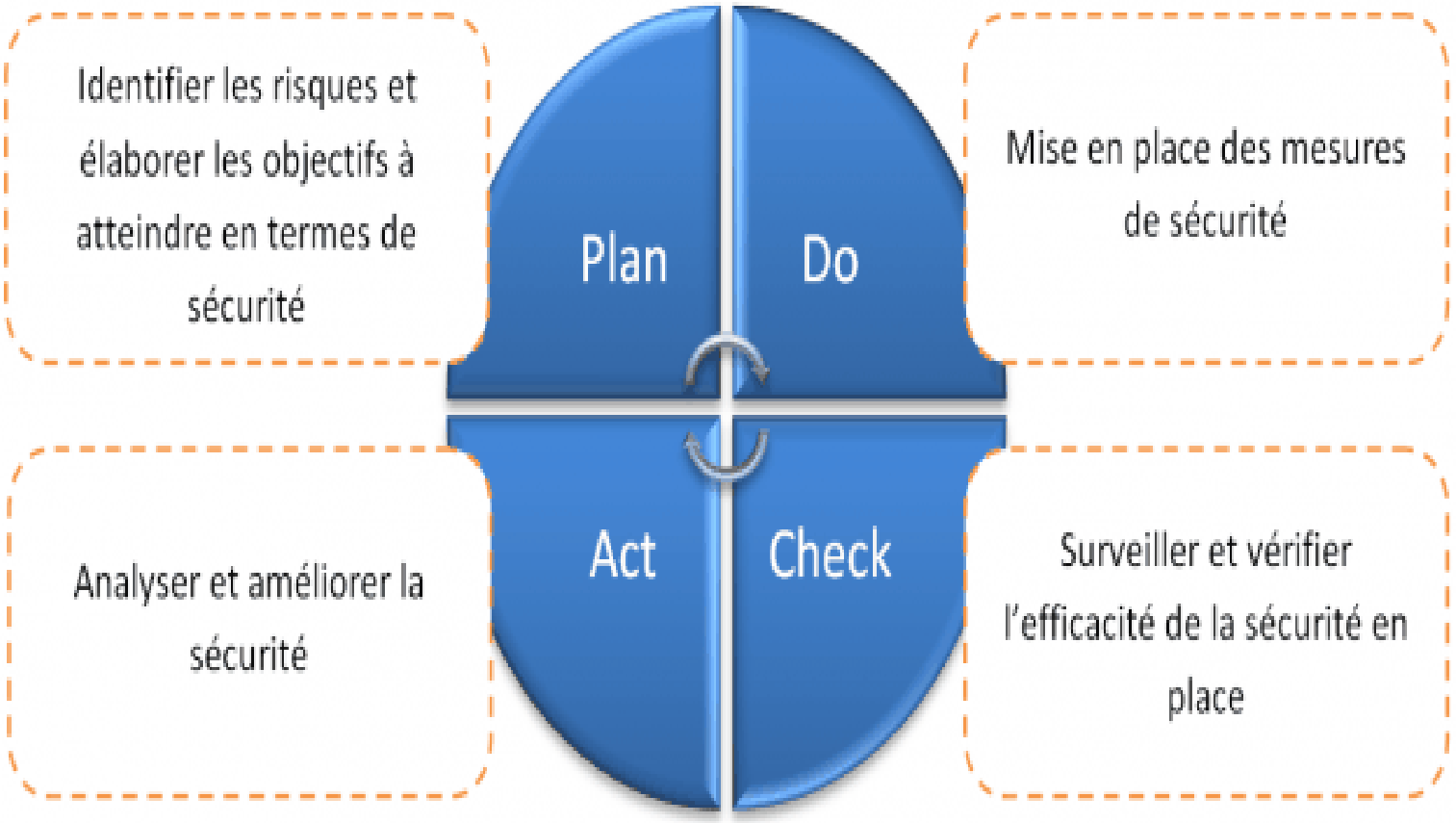
- Management System : Système pour établir la politique et les objectifs et pour atteindre ces objectifs (ISO guide 72).
- Les systèmes de management sont utilisés dans les entreprises pour développer leurs politiques et les mettre en application à travers des objectifs et des cibles en utilisant:
  - Une organisation dans l'entreprise,
  - Des processus et des ressources associés,
  - Des contrôles et une méthode d'évaluation,
  - Des processus de révision pour garantir que les anomalies sont corrigées et mettre en œuvre des axes d'amélioration le cas échéant.

Système de Management de la Sécurité de l'Information (2)

- Certaines organisations commencent à aborder la sécurité de l'information comme un système intégré appelé Information System Management System (ISMS).
- Mise en œuvre d'un vrai processus d'analyse, d'élaboration de contrôle et d'évolution d'une politique de sécurité en appliquant un concept bien connu en qualité, le modèle PDCA (Plan Do Chack Act).

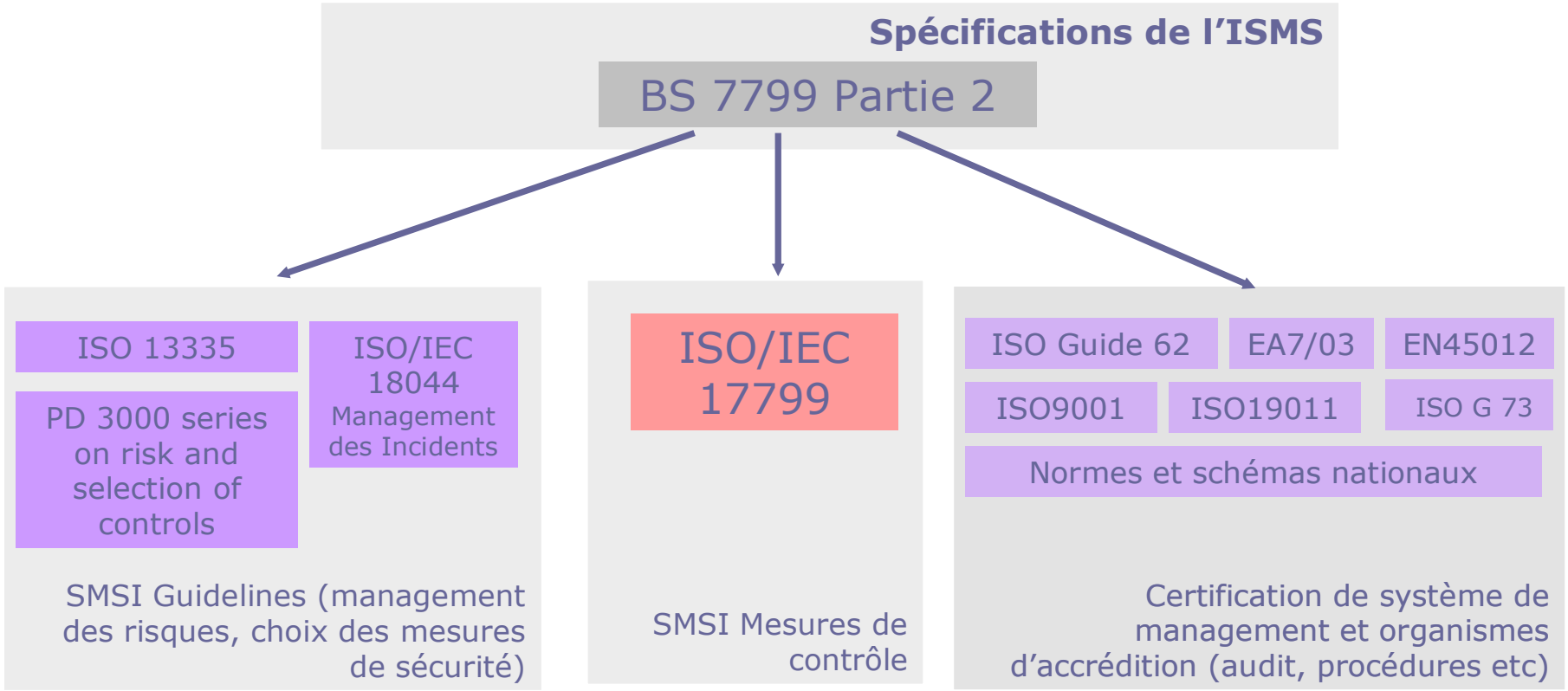
Système de Management de la Sécurité de l'Information (3)

- Modèle PDCA.



Système de Management de la Sécurité de l'Information (4)

- Les normes pour construire un SMSI.



La certification BS7799-2

- A l'instar de ISO 9000 pour le management de la qualité, BS 7799-2 est la seule norme et certification qui existe actuellement pour les ISMS.
- Définit les conditions pour l'établissement, la mise en œuvre et la documentation d'un ISMS,
  - Définit les exigences de contrôles pour la sécurité devant être mis en application selon les besoins de différents organismes,
  - Elle se compose de 10 chapitres de 127 contrôles,
  - Nécessite 2 étapes (audit de la documentation puis audit de l'implémentation),
  - En France, le COFRAC (Comité Français d'Accréditation et de Certification) peut valider un schéma de certification BS 7799-2.

Conclusion

Actuellement, l'informatique est partout, il est donc très dur de se protéger face aux pirates qui sont de plus en plus nombreux et qui se développent souvent. Le nombre de piratage augmentent, ainsi que les techniques qui sont de plus en plus rapides et efficaces. En effet, même si les pirates informatiques ont un avantages en technique, certains pirates contribuent à la sécurité d'autrui sur internet et autres réseaux sociaux. On peut donc en déduire que la sécurité informatique avance grâce au piratage. Les deux sont liés, donc un jour, peut-être que la sécurité contrera le piratage mais pour le moment, le piratage est omni-présent alors que la sécurité l'est peu.

Le proverbe dit : « Mieux vaut prévenir que guérir. » Au terme du parcours des divers aspects de la sécurité des systèmes d'information, nous pouvons dire qu'en ce domaine prévenir est impératif, parce que guérir est impossible et de toute façon ne sert à rien. Lorsqu'un pirate a détruit les données de l'entreprise et que celle-ci n'a ni sauvegarde ni site de secours, elle est devenue condamnée ce qui implique l'organisation de travailler avec une politique de sécurité.