Innovations numériques et cybercriminalité: défis et risques

Adel Jomni
Enseignant-chercheur
Université de Montpellier

Brève présentation

ADEL JOMNI

- Enseignant-chercheur (Université de Montpellier)
- Expert auprès du Conseil de l'Europe
- Directeur diplôme d'université : Cybercriminalité : Droit, Sécurité de l'information & Informatique légale
- Co-directeur du diplôme d'Université: DPO: Droit et management de la sécurité des donnés
- Membre du comité scientifique du Forum International sur la Cybersécurité (FIC)
- adel.jomni@umontpellier.fr

Objectifs

- Identifier les principales tendances et innovations numériques et les risques inhérents
- Comprendre les principales menaces cybercriminelles et leurs modes opératoires
- S'informer sur les dispositifs juridiques réprimant la cybercriminalité

Contenu du cours

Partie1: Principales innovations numériques et risques inhérents

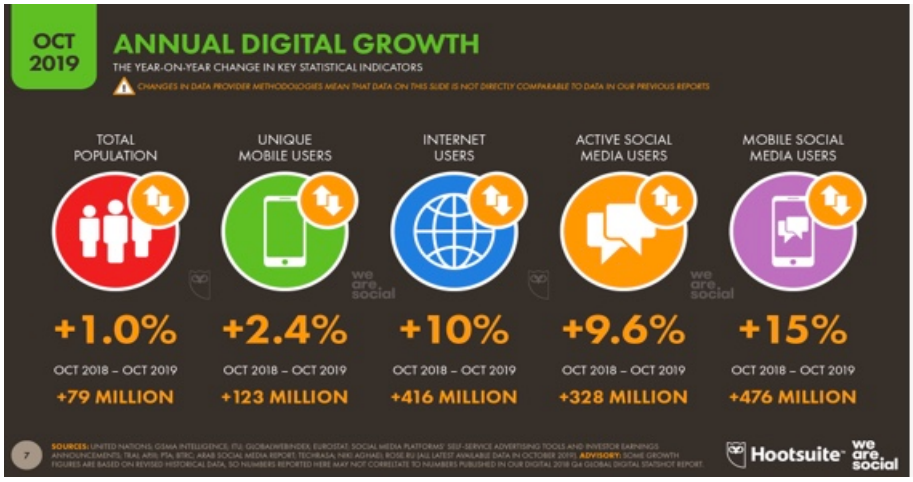
Partie2: Cybercriminalité: principales infractions, modes opératoires et dispositifs juridiques

La société de l'information

Statistiques (Octobre 2019)

Source: https://wearesocial.com/fr

Evolution en un an



Une croissance annuelle de 10 % du nombre d'internautes.

Statistiques en France

- 92 % de la population utilise Internet, soit une hausse de 5,5 % sur un an
- 74 % de la population se connecte régulièrement sur mobile.
- En moyenne 4 h 38 chaque jour.
- 71 % déclarent avoir acheté un produit ou service en ligne au cours du dernier mois, dont 26 % sur mobile.
- Sur leurs smartphones, les utilisateurs français installent en moyenne 98 applications et en utilisent 34 au moins une fois par mois.
- Facebook truste largement le classement de ces apps : l'application du réseau social Facebook est la plus utilisée, suivi de ses messageries Messenger, Whatsapp et Instagram.

Usages du numérique en France

- 4 personnes sur 5 ont un usage quotidien d'internet, soit une augmentation de 4% depuis 2017.
- les 70 ans et plus sont désormais 60% à utiliser internet contre 38% en 2015.
- La proportion d'internautes (70 ans et +) quotidiens a doublé sur la même période, passant de 22% à 45%. (source ARCEP). +7% en 2018.

Risques !

Caractéristiques de la nouvelle société de l'information

- L'information prend une nouvelle dimension: ouverte et chacun peut y accéder
- Il n'y a plus de distance physique entre les gens, où qu'ils se trouvent. L'information est partout et tout le temps
- Le cyberespace n'est pas concerné par les frontières politiques
- Les informations et les connaissances peuvent être obtenues librement et démocratiquement

Transformation numérique (digitale)

- Elle désigne les changements liés à l'intégration des innovations technologiques dans la société en général et dans les organismes publics et privés en particulier.
- L'académicien Michel Serres évoque la digitalisation comme « la troisième révolution anthropologique majeure », preuve de son importance sur la société actuelle.
- **1ère révolution:** passage de l'oral à l'écrit
- **2ème révolution:** apparition de l'imprimerie, au XVIe siècle

Technologies innovantes

Véritable révolution technologique à la base des dernières innovations numériques

- Cloud computing
- Big Data
- Intelligence artificielle / machine learning
- Internet des objets (IoT)
- Impression 3D
- Blockchain et cryptomonnaies
- ....

induisent une transformation «importante» dans l'usage des technologies de l'information par les entreprises et par les individus

Cloud Computing (Informatique en nuage)

- C'est incontestablement l'évolution majeure des technologies informatiques de ces dernières années.
- Couvre un concept technique et des offres de services multiformes.
- Permet de fournir de l'informatique sous forme de services et non de produits
- Les dépenses des entreprises dans l'univers du Cloud augmentent chaque année de 20%
- Les dépenses mondiales consacrées au Cloud devraient augment de 100% lors des 5 prochaines années (de 229 milliards de dollars en 2019 à 500 milliards)

3 principaux services

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Avantages du Cloud computing

- Focaliser les ressources de l'entreprise sur le management et l'aspect business
- Meilleure prise en charge des évolutions technologiques (pas d'installation ni de mises à jour, montée en charge automatisée,..)
  - Pas besoin d'investir dans une infrastructure physique.
  - Faciliter le développement des applications.
  - Flexibilité / Adaptabilité
  - Favoriser le travail collaboratif
- Meilleure maîtrise des budgets associés à l'informatique: modèle de prix basé sur la demande et l'utilisation
- Extensibilité/ Mobilité
- Rèpondre à la pénurie des compétences dans certains domaines IT
- Sécurité physique du matériel

Cloud computing: Risques et Sécurité

La « sécurité » est souvent citée comme le frein principal à l'adoption des services Cloud. Elle concerne essentiellement la confidentialité et l'intégrité des données:

- **Risques liés aux choix techniques du prestataire**
- **Risques liés à la perte de maitrise de son système d'information**

- La concentration de données potentiellement sensibles sur des serveurs risquent d'attirer les hackers.
- Investigation: Impossibilité d'assurer la traçabilité des données

La protection des données est la problématique la plus anxiogène du Cloud !!

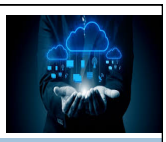
Exemples d'attaques …

- **Des données du Pentagone stockées sur AWS accessibles publiquement**
  - A travers Amazon Web Services, le Pentagone a laissé pendant des mois, voire des années, l'accès public à des milliards de données collectées en ligne.
    - Source https://www.silicon.fr/donnees-pentagone-stockees-aws-190971.html?inf_by=5a43d377671db8c10a8b4a9
- **Accenture victime d'une fuite de données à la suite de l'exposition de plusieurs espaces de stockage AWSS3**
  - Source https://www.cyberveille-sante.gouv.fr/cyberveille/244-accenture-potentiellement-victime-dune-fuite-de-donnees-suite-lexposition-de

La protection des données personnelles hébergées dans le Cloud est devenue un véritable enjeu.

- Patriot Act : loi antiterroriste autorisant les services de sécurité US à accéder aux données informatiques détenues par les particuliers et les entreprises, sans autorisation préalable d'un juge et sans en informer les utilisateurs.

Risques juridiques liés à la localisation des données



Extraterritorialité du droit

- Les questions du droit applicable et de la juridiction compétente
- difficultés inhérentes à
  - la saisine de tribunaux situés à l'étranger,
  - des coûts de procédures très élevés

Données personnelles, RGPD et Cloud Computing

- Le RGPD (Règlement Général sur la Protection des Données ou GDPR en Anglais): est une directive européenne obligeant toute entreprise ou administration à respecter certaines règles lorsqu'il doit traiter des données personnelles
- Le RGPD a pour but de coordonner toutes les règles actuellement en vigueur par rapport aux données personnelles en Europe. Il a par conséquent une incidence directe sur le Cloud et la façon dont les différents fournisseurs gèrent ces données.
- Il est entré en application directe le 25 mai 2018 sur tout le territoire de l'Union Européenne.
  - Le stockage des données doit répondre à un certain nombre de normes restrictives fixées par le RGPD (interopérabilité, minimisation, etc)
  - La maîtrise de la chaîne de sous-traitance de l'hébergeur
  - L'économie des APIs ne pourra pas faire l'impasse du RGPD.

Recommandations CNIL

- la CNIL a constaté que les utilisateurs de cloud souffrent d'une insuffisance de transparence de la part des prestataires (conditions de réalisation des prestations, sécurité, éventuel transfert à l'étranger des données, etc.)
- Avant de recourir à un service de cloud computing, la CNIL recommande de réaliser une analyse de risques et d'être très rigoureux dans le choix de son prestataire.
- La CNIL propose des modèles de clauses de confidentialité.
- https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

RGPD et sanctions

- En cas de manquement, les fournisseurs de solutions de cloud ou les entreprises peuvent être contraints de payer des amendes sur les chiffres d'affaires.
- Ce montant peut grimper à 4 % du chiffre d'affaires mondial ou atteindre les 20 millions d'euros en cas de refus d'obtempérer face aux injonctions de la CNIL, en cas de traitements de données illégaux, de défaut de consentement, de manque de prudence lors des transferts transfrontaliers de données ou encore de non-respect des droits des personnes
- En dehors de l'aspect financier, le manquement au respect du RGPD pourrait avoir sur l'image d'une entreprise.
- Un déficit de confiance peut être très préjudiciable

CaaS (Crime as a Service): Le cybercrime comme un service

- La majorité des Cyberdélinquants n'a pas les connaissances et/ou les capacités nécessaires à la création de logiciels malveillants.
- Les cybercriminels sont si bien organisés qu'ils achètent désormais « clef en main » les kits d'exploits et logiciels qu'ils utilisent pour mener à bien leurs activités.

Technologies innovantes

Véritable révolution technologique à la base des dernières innovations numériques

- Cloud computing
- Big Data
- Internet des objets (IoT)
- Intelligence artificielle / Machine learning
- Blockchain - cryptomonnaies
- ....

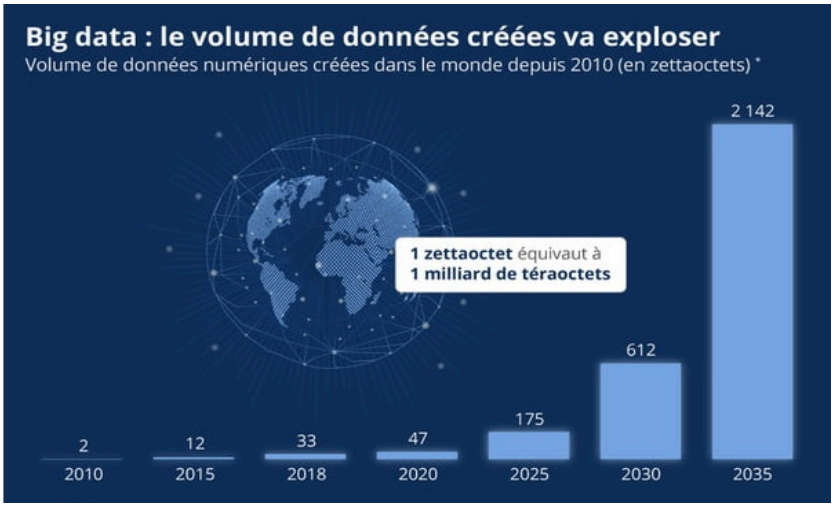
induisent une transformation «importante» dans l'usage des technologies de l'information par les entreprises et par les individus

BIG DATA (mégadonnées)

Désigne de gros volumes de données (structurées et non structurées) provenant de sources numériques (interne et externe à l'entreprise) très difficiles à traiter et exploiter avec les outils classiques de gestion de bases de données.

- Le volume des données double tous les deux ans.
- 90% des données existantes aujourd'hui ont été créées au cours des deux dernières années et la production de celles-ci devrait exploser de 800% d'ici 5 ans, selon les prévisions du cabinet Gartner.
- Fin 2018, le volume mondial de données numériques atteignait 33 zettaoctets. Il dépassera les 610 en 2020. Le volume de données mondial sera multiplié par 45 entre 2020 et 2035

Volumes des données entre 2010 et 2035



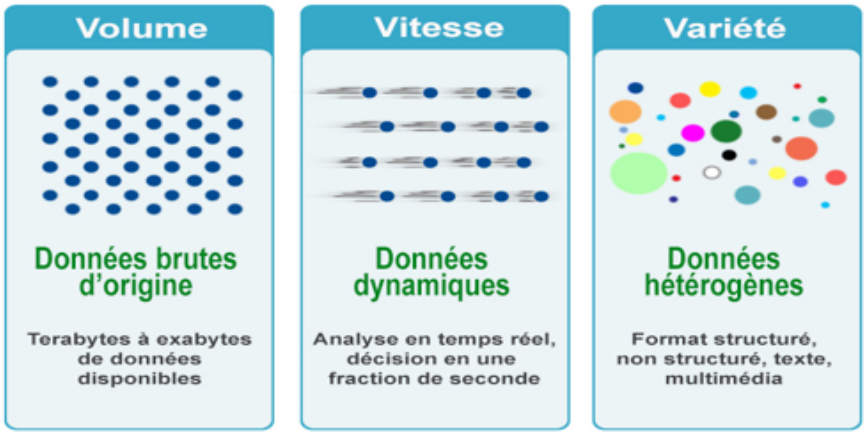
Source: Statista

BIG DATA (mégadonnées)

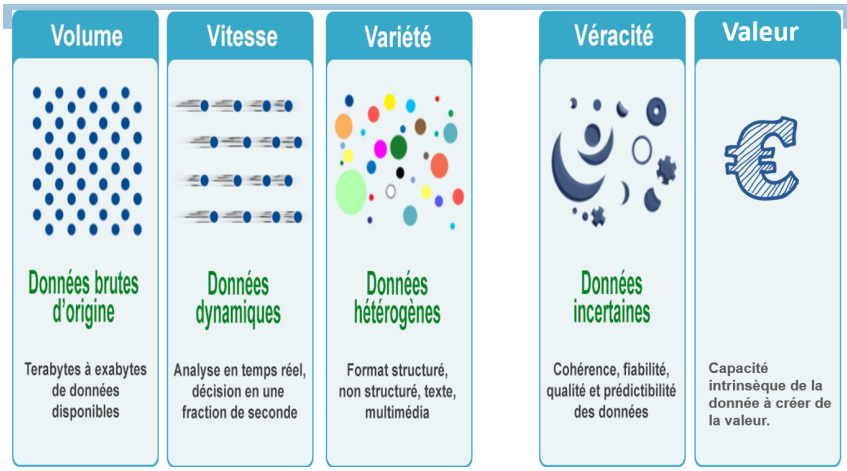
- BIG DATA vise à convertir cet important volume de données en informations et connaissances qui peuvent aider les professionnels de santé et les chercheur pour:

BIG DATA= DATA (données) + innovation technologiques pour faciliter le stockage et l'analyse des données

BIG DATA : 3V



BIG Data: 5V



BIG DATA et Risques

- le Big Data, avec la constitution de grands réservoirs de données attirent les Cyberdélinquants , d'autant que le volume des données ne va pas cesser d'augmenter avec l'arrivée des objets connectés et la généralisation des mobiles intelligents.

BD est un nouveau paradis pour les cyber-attaquants et également pour certains gouvernements

BIGDATA et risques sur la vie privée

Exemple du programme Programme PRISM

- Le programme américain de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques (Géants du Web).
- la NSA disposerait d'un accès direct aux données hébergées par les géants américains des nouvelles technologies

BIG DATA et RGPD

- la constitution d'un Data Lake ignore souvent les principes prônés par le RGDP !!
  - Minimisation (…*les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire en lien avec la finalité pour laquelle les données sont traitées*).
  - limitation de la durée de conservation des données (…*le responsable du traitement garantisse une durée de conservation des données qui soit limitée au strict minimum*)

Cybercriminalité et Big Data : l'impact des technologies analytiques sur la sécurité

Dans un futur proche, grâce à l'analyse prédictive, il sera possible de prédire quelques cyberattaques ou des attaques terroristes en combinant:

- activités sur les réseaux sociaux
- des recherches sur le réseau Internet
- des achats effectués sur Internet
- la géolocalisation des smartphones.
- communications téléphoniques
- navigations Internet
- Drones / Caméras vidéos

Détection des signaux faibles

Technologies innovantes

Véritable révolution technologique à la base des dernières innovations numériques

- Cloud computing
- Développement AGILE
- Big Data
- Intelligence artificielle / Machine learning
- Internet des objets (IoT)
- Blockchain
- ....

induisent une transformation «importante» dans l'usage des technologies de l'information par les entreprises et par les individus

Intelligence artificielle (IA)

- Science qui a pour but de faire faire par une machine des tâches que l'homme accomplit en utilisant son intelligence.
- L'IA est l'étude des concepts qui permettent de rendre les machines intelligentes.
- l'IA s'intéresse à tous les cas où un traitement informatique ne peut être ramené à une méthode simple, précise, algorithmique : exemple faire un diagnostic (médical, de défaillance, ...).

Exemple le programme Watson d'IBM

Watson exploite l'IA pour aider de nombreux secteurs d'activité comme la finance, la santé, le secteur public, le commerce, l'éducation et l'assurance à se transformer.

- **SANTE**
  Watson révolutionne le secteur de la santé en aidant la recherche et les diagnostics dans le domaine du Cancer
- **FINANCE**
  IBM aide ses clients à utiliser l'IA pour mieux gérer les risques et proposer des conseils personnalisés et des options d'investissements adaptées.

Big Data et Intelligence artificielle au service de l'investigation criminelle: Exemple: AnaCrim

- Logiciel utilisé par la police judiciaire afin de:
  - *avoir une vision globale de la procédure et de distinguer la logique qui se dessine au travers de la commission d'un fait criminel ou délictuel*
  - croiser tous les indices recueillis.
  - identifier les liens entre différentes entités, même si elles n'ont pas de rapport évident entre-elles
  - mettre en évidences les incohérences d'un témoin ou d'un mis en cause, des contradictions entre certains témoignages et les observations faites par les enquêteur.
- Un Magistrat référent est chargé de contrôler la mise en œuvre de ces logiciels.
- Les traitements sont opérés sous le contrôle du procureur de la République compétent.

Open data: Algorithmes et l'IA font leur entrée dans les tribunaux: « émergence de la justice prédictive ».

- Disposition de la loi République Numérique du 7 octobre 2016: toutes les décisions de justice doivent désormais être accessibles en ligne (anonymisées).
- On estime leur nombre à environ 4 millions chaque année.
- Anticiper le sens des décisions de justice.

Les algorithmes font leur entrée dans les tribunaux: « "émergence de la justice prédictive"

- Disposition de la loi République Numérique du 7 octobre 2016: toutes les décisions de justice doivent désormais être accessibles en ligne (anonymisées).
- On estime leur nombre à environ 4 millions chaque année.

- Justice prédictive: anticiper le sens des décisions de justice.

Quelle éthique pour les algorithmes dans l'IA ?

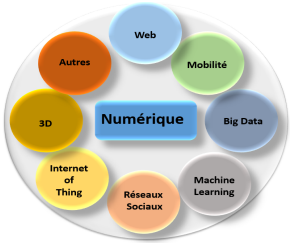
- Les commerçants rêvent de trouver l'algorithme qui saura proposer les produits auxquels leurs clients n'ont pas encore pensé, mais qu'ils vont adorer.
- Les manipulateurs en tout genre cherchent activement l'algorithme qui vous connaîtra mieux que vous-même.

- La CNIL réfléchit sur ce thème avec la recommandation de former à l'éthique tous les maillons de la chaîne algorithmique (concepteur, professeurs, citoyens).
- On imagine sans peine l'impact qu'une telle formation peut avoir sur les spécialistes de la manipulation.

Technologies innovantes

Véritable révolution technologique à la base des dernières innovations numériques

- Cloud computing
- Développement AGILE
- Big Data
- Intelligence artificielle / Machine learning
- Internet des objets (IoT)
- Blockchain
- ....



induisent une transformation «importante» dans l'usage des technologies de l'information par les entreprises et par les individus

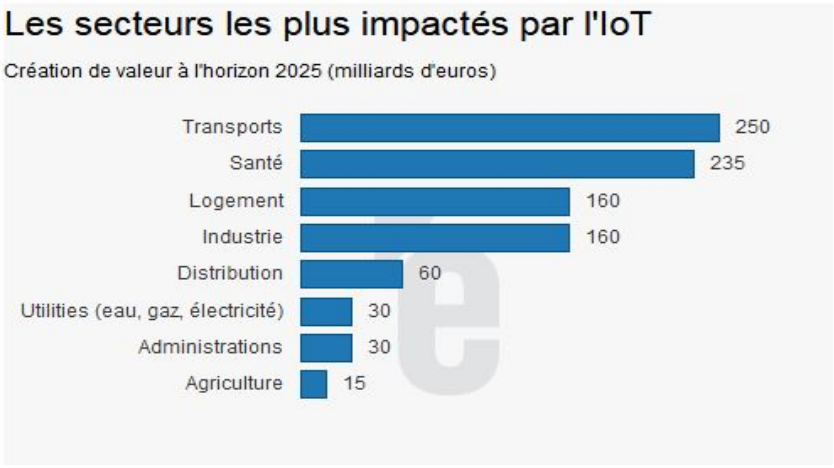
Internet des objets (ou Internet of Things-IoT)

- Plusieurs objets pouvant communiquer, entre eux, et avec le reste du réseau Internet.
- Cette extension d'Internet à des « objets » physiques est appelée l'Internet des Objets.
- L'internet des objets revêt un caractère universel et vise des usages variés comme la e-santé , la domotique, les loisirs, le transport, la sécurité, le Quantified self …

Evolution du WEB

- WEB 1.0
- WEB 2.0
- WEB 3.0
- WEB 4.0

Impacts



Source AT Kearney

Quelles perspectives pour l'IoT?

Couplé avec le développement du Cloud computing, Big Data et de l'intelligence artificielle, l'IoT peut créer de nouveaux services ou améliorer des services existants.

Exemples:

- Améliorer le traitement des pathologies
- améliorer le confort et de faciliter la conduite (l'assistant de parking)
- le suivi de la consommation et de l'usure des pièces,
- le dépannage,
- la gestion du trafic et la simplification des déplacements.

IoT et sécurité

En dépit des opportunités qu'elle génère, le principal frein à une adoption massive de ces technologies est la sécurité.

Parmi les risques de sécurité potentiels, on note :

- Écoute clandestine des communications
- Accès non autorisé / vol des données
- Modification/falsification de données
- Déni de service
- Accès physique aux capteurs
- Le manque de contrôle de ses propres données à cause d'une dissémination dans plusieurs applications

Objets connectés et sécurité des entreprises

- Augmentent la surface d'attaque soit par les employés qui les amènent soit par l'entreprise qui les utilise
- Pas conçus pour l'entreprise, ils ne suivent presque jamais la politique de sécurité du SI, malgré le fait qu'ils peuvent se connecter au réseau de la société.
- l'exfiltration de données confidentielles de l'entreprise par un objet connecté apporté par un employé ou se trouvant dans l'entreprise.

Objets connectés: une opportunité pour l'investigation et les enquêtes criminelles

- Les objets connectés présentent de nombreuses opportunités pour les activités des forces de sécurité, que ce soit pour la sécurité publique, la police judiciaire ou le renseignement.
- dispositifs mis en œuvre dans le cadre de techniques spéciales de surveillance (balises, dispositifs de sonorisation, drones, etc.).
- l'exploitation des objets connectés utilisés par des victimes ou par des criminels (montres GPS, pacemakers, bracelets connectés Fitbit...)

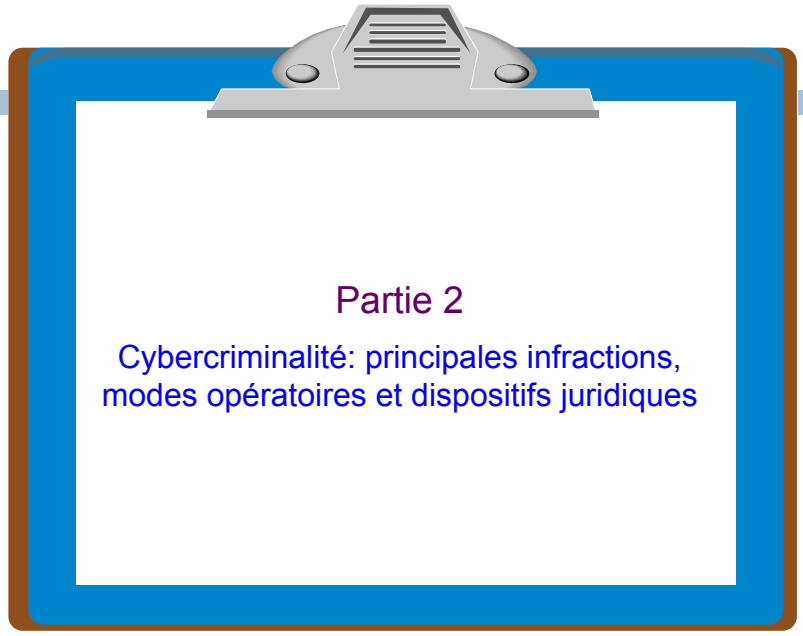
IoT et RGPD

- Les données collectées par les OC sont une source de violation de la protection des données à caractère personnel (montres, jouets, téléviseurs, Linky (compteur) , voitures, drone, assistants vocaux, enceintes, etc)
- RGPD impose de nouvelles contraintes à l'IoT: Nécessité de prendre en compte le RGPD dès la conception et la collecte des données (sécurité, données minimales, exercice de certains droits (information, rectification, effacement, portabilité..), traçabilité, etc)

Intégrer le Privacy by Design

IoT: le défi de la sécurité- Recommandations

- Privacy by design
- Security by design



Partie 2

Cybercriminalité: principales infractions, modes opératoires et dispositifs juridiques

Innovations numériques et défis pour la sécurité

- Les innovations numériques offrent au quotidien une multitude d'expériences et de services intéressants
- Elle offrent en même temps des opportunités nouvelles pour les Cyberdélinquants notamment dans le domaine économique et financier.
- Elles ont engendré une nouvelle forme de délinquance : la cybercriminalité ou Cyberdélinquance.
- De nouveaux risques et menaces ont émergé ou parfois se sont généralisés.

La Cybersécurité est désormais un facteur de compétitivité essentiel pour chaque entreprise.

Cybersécurité

Etat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense » (Définition de l'ANSSI)

Les enjeux de la cybersécurité

Pour les Etats : souveraineté nationale

- Stratégique (une problématique de défense et sécurité nationale)
- Diplomatique
- Economique
- Militaire
  - ✓ déstabiliser l'ennemi en portant atteinte, voire en détruisant ses systèmes informatiques.

✓ Le cyberespace devient un lieu d'affrontements géopolitiques.

✓ La cyberdissuasion est devenue une nouvelle doctrine de défense nationale.

Les enjeux de la cybersécurité

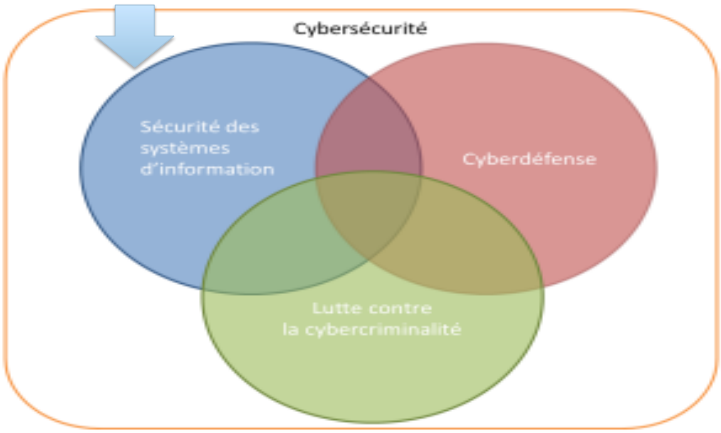
Pour les entreprises

- Financier (perte de chiffre d'affaires, perte d'avantage concurrentiel...)
- Juridique (amendes, non respect des libertés individuelles…)
- Perte d'image (réputation, confiance des clients…)

Pour les citoyens,

- protéger ses données personnelles et sa vie privée.

Cybersécurité



Sécurité des systèmes d'information (SSI)

Est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information »

L'objectif est de prévenir les menaces et d'assurer la disponibilité, la confidentialité et l'intégrité d'un système d'information.

Disponibilité d'un SI

Disponibilité

- fait référence à la possibilité d'accéder à une ressource dans un SI.

Confidentialité

- consiste à limiter l'accès aux ressources (données) d'un SI à des personnes (ou programmes) autorisées.

Intégrité

- fait référence à la fiabilité d'une ressource.

Cyberdéfense

Ensemble des mesures techniques et non-techniques permettant à un État de défendre, dans le cyberespace, les systèmes d'information jugés essentiels

La cyberdéfense: enjeu mondial, une priorité nationale

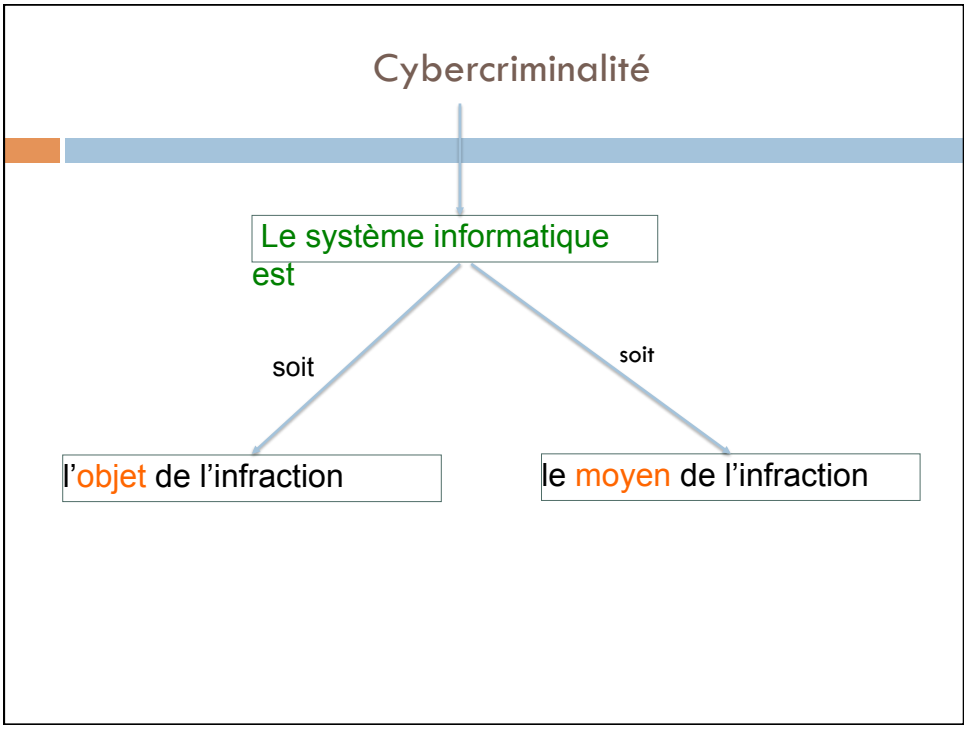
Cyber-terrorisme

- Utilisation de l'information et du contrôle des systèmes d'information, par des groupes organisés ou par un individu, comme arme stratégique pour exercer des pressions et intimider l'adversaire.
- Il se manifeste essentiellement par de manipulation de l'information, de désinformation, de piratage, d'infiltration de réseaux, etc.
- Le Déni de service (DDoS) est un exemple type d'attaque qui peut être utilisée à des fins cyberterroristes.
- La manipulation de l'information est une forme de cyberterrorisme

La cybercriminalité: Définition

Selon la commission européenne, la cybercriminalité englobe trois catégories d'activités criminelles :

- Les infractions propres aux réseaux électroniques (déni de service et piratage)
- Les formes traditionnelles de criminalité (escroquerie, vols de données , fraudes, fausses cartes de paiement , usurpation d'identité en ligne)
- La diffusion de contenus illicites (pédopornographie , racisme, xénophobie)



Quelques chiffres

- La cybercriminalité est devenue la troisième plus grande menace à la stabilité mondiale
- 43% des cyberattaques visent les petites entreprises.
- 4 PME sur 10 (42%) ont déjà subi une ou plusieurs attaques ou tentatives d'attaques informatiques.
- En France, 8 entreprises sur 10 sont touchées par des cyber attaques chaque année.
- Les principaux types d'attaque : hameçonnage (24 %) ; malware (20 %) ; rançongiciel (16 %) ; fraude au président (6 %).

Sources : Cesin, Symantec, Small Business Trends, CPME, ZDNet, IBM, Varonis, Gallup, IT Governance, Accenture, Cibersecurity Ventures, Juniper Research, Clusif, L'Usine Nouvelle, Le Monde numérique.

Cyberattaques et Conséquences sur le système bancaire

(enquête publiée en janvier 2020)

- La Federal Reserve System (FED) a évalué les conséquences qu'une cyberattaque aurait sur le système bancaire:
  - dans l'hypothèse où les institutions américaines seraient visées par une cyberattaque de grande envergure, plus d'un tiers des actifs bancaires pourrait être affecté.
  - Les banques pourraient perdre l'équivalent de 2,7 fois le PIB des États-Unis.
  - une cyberattaque pourrait déclencher une course à la liquidité et entraîner des problèmes de solvabilité.
  - même une cyberattaque visant des banques ayant moins de 10 milliards de dollars d'actifs porterait atteinte à une partie importante du système bancaire américain et mondial.

Cyberattaques, Anatomie d'une Cyberattaque

- Renseignement et préparation
- Conception
- Infiltration et exploration
- Contrôle et commande
- Collecte
- Monétisation

Impacts

66

Il peut prendre plusieurs formes:

- Perte de crédibilité;
- Perte financière;
- Détérioration de la réputation ou de l'image de marque de l' organisation,..
- Blocage de sites d'importance vitale pour un Etat

La cybercriminalité constitue l'une des formes de criminalité transnationale qui connaît le développement le plus rapide dans les pays membres d'INTERPOL.

Menaces

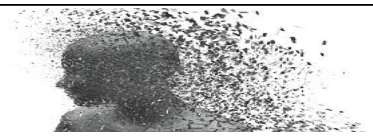
- Désignent l'ensemble des éléments (internes et/ou externes) pouvant atteindre le SI d'une organisation.
  - Menaces d'origine humaine *(fuite, malveillance, espionnage, vol, etc.)*.
  - Menaces d'origine technologique *(spam, virus, ver, keyloggers, cheval de troie, Phishing, Botnets, Rootkit, RAT, DDoS, etc.)*

Vulnérabilités

- Traduisent toutes les faiblesses des ressources du SI qui pourraient être exploitées par des **menaces,** dans le but de compromettre le bon fonctionnement du SI.

- Elles peuvent être de plusieurs types:
  - Humaine,
  - Technologique,
  - Organisationnelle

Vulnérabilités humaines



Social engineering (ingénierie sociale) - Exemple des Fovis
Arnaques aux sentiments
La Pédopornographie
Le "Revenge porn" ou la vengeance pornographique
Phishing (hameçonnage) ou vol d'identité
La revente des données de l'entreprise
La connexion d'une clé USB inconnue
Les téléchargements et streaming non protégés
La négligence

Vulnérabilité humaine: l'exemple du Social engineering (ingénierie sociale)

70

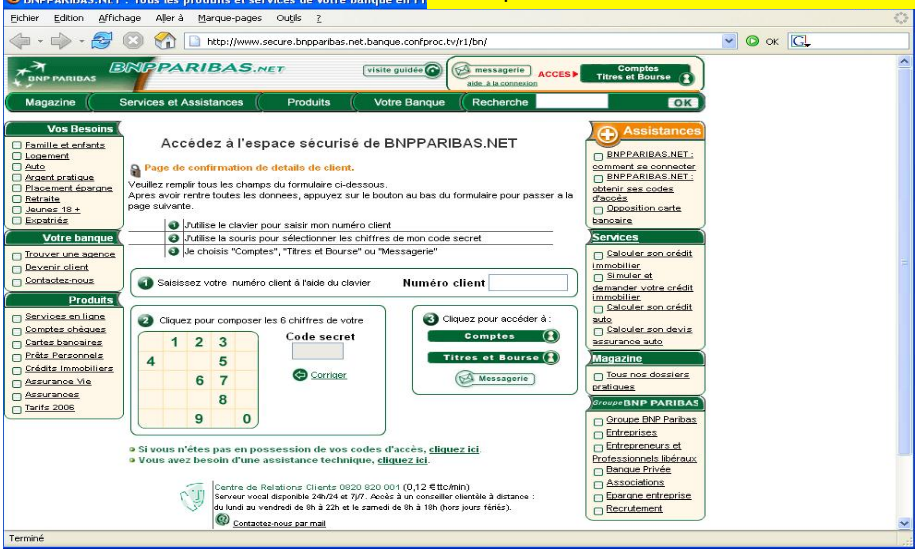
- C'est une technique de manipulation par tromperie qui vise à obtenir l'accès à des informations confidentielles par la manipulation de personnes en ayant directement ou indirectement l'accès.
- Le facteur humain est le point central des techniques d'attaque rencontrées en social engineering. Des relations de confiance ne reposant sur rien de concret sont mises en place de manière calculée mais le plus souvent par simple discussion, et exploitées par la suite pour tirer un maximum de profit de la situation.

Phishing (hameçonnage) ou vol d'identité

71

- Technique de manipulation par tromperie qui vise à obtenir l'accès à des informations confidentielles (exemples: numéros de cartes bancaires, des identifiants de connexions, des mots de passe pour des services de commerce en ligne, etc.)
- **L'usurpation d'identité** est l'objectif principal de cette menace.
- En 2018, le phishing (ou hameçonnage) est le mode d'attaque le plus fréquent avec 73% d'entreprises touchées.

L' extension .**tv est en fait le domaine officiel de** Tuvalu, une île qui se situe dans l' Océan
Pacifique entre Hawai et l' Australie



Spear phishing

- une variété du phishing
- il cible une personne spécifique, ou les cadres d'une entreprises spécifique pour des attaques majeures contre les grandes entreprises, les banques ou les personnes influentes.
- les cybercriminels rassemblent des informations sur la victime de manière méticuleuse pour que l' » appât » soit encore plus appétissant.
- deux motifs se cachent derrière le spear phishing : voler de l'argent et/ou des secrets.

Phishing: sanctions pénales

Usurpation d'identité,

- depuis la loi LOPSI II du 14 mars 2011, le « phishing » rentre dans le champ de la nouvelle incrimination relative à l'usurpation d'identité en ligne, que l'article 226-4-1 de Code pénal punit d'un an d'emprisonnement et de 15 000 € d'amende.

Escroquerie,

Sur le fondement de l'article 313-1 du Code pénal, qui punit de 5 ans d'emprisonnement et de 375 000 € d'amende « le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque […] ».

Phishing: Suite des sanctions

Contrefaçon de droits intellectuels (pages Web, marques, logo, chartre graphique..),

Sur le fondement des articles L. 713-2 et L. 713-3 du Code de la propriété intellectuelle. Le propriétaire du site reproduit ou imité par le « phisheur » peut ainsi faire sanctionner l'usage de sa marque sur le fondement de la contrefaçon. Le délit de contrefaçon est passible de 3 ans d'emprisonnement et 300 000 € d'amende.

Collecte frauduleuse de données à caractère personnel,

Sur le fondement de l'article 226-18 du Code pénal, qui prévoit une peine de 5 ans de prison et de 300 000 € d'amende.

Atteinte à un système de traitement automatisé de données,

Sur le fondement de l'article 323-3 du Code pénal, qui punit de deux ans d'emprisonnement et 30 000 € d'amende « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ».

Typosquatting

- Une technique consistant à acheter des noms de domaine qui ressemblent étrangement à des noms de site connus, mais avec des fautes volontaires, comme des erreurs orthographiques.
- Ces achats peuvent être considérées comme des actes préparatoires à des attaques de type spear-phishing (campagne de faux emails ciblée)
- le typosquatting permettant de mettre en confiance les destinataires avant de les tromper.

LA PÉDOPORNOGRAPHIE

- La pédopornographie par Internet constitue une forme particulièrement grave d'exploitation sexuelle des enfants. A ce jour, on compte environ 100000 sites consacrés à la pédopornographie.

- La pornographie infantile, ou pédopornographie, est définie par les Nations unies comme «toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles».
- Les affaires de pédophilie représentent, en France, environ 20 à 40% des affaires pénales touchant Internet chaque mois.

Pédopornographie: sanctions pénales

Les auteurs qu'il s'agisse des producteurs, d'intermédiaires ou de simples consommateurs d'images de mineurs à caractère pornographique peuvent faire l'objet de poursuites pénales sur différents fondements juridiques.

- L'article 227-23 du code pénal sanctionne de cinq ans d'emprisonnement et de 75000€ d'amende «le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image présente un caractère pornographique».
- Il en est de même du «fait de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter».
- Les peines sont portées à 7 ans d'emprisonnement et à 100000€ d'amende lorsque la diffusion de ces images s'est faite sur un réseau de télécommunication tel qu'internet.
- Le simple fait de détenir une telle image, ou représentation, est puni de deux ans d'emprisonnement et 30 000 euros d'amende.

Pédopornographies- sanctions pénales suite

La représentation à caractère pédophile inclut les montages et dessins à caractère pédophile fabriqués à partir de photographies d'enfants, mais aussi les images à caractère pédophiles totalement virtuelles.

Ces dispositions sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée d'au moins 18 ans au jour de la fixation ou de l'enregistrement de son image. Il existe donc une présomption de minorité qui fait peser la charge de la preuve sur le détenteur des images.

- Est également sanctionné le fait de faire des propositions sexuelles à un mineur par un moyen de communications électroniques. Ainsi, «le fait pour un majeur de faire des propositions sexuelles à un mineur de 15 ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de 2 ans d'emprisonnement et de 30000€ d'amende». Les peines sont d'ailleurs aggravées à 5 ans d'emprisonnement et 75000€ d'amende lorsque les propositions aboutissent à une rencontre.

Loi du 7 octobre 2016 pour une République numérique – Incrimination du « revenge porn »

- L'incrimination de la vengeance pornographique (*revenge porn*) résulte de la loi du 7 octobre 2016 pour une République numérique qui modifie l'article 226-1 du Code pénal. Est puni de deux ans d'emprisonnement et de 60 000 euros d'amende le fait de transmettre ou de diffuser sans le consentement exprès de la personne l'image ou la voix de celle-ci, prise dans un lieu public ou privé, dès lors qu'elle présente un caractère sexuel.

- La diffusion d'images intimes d'un(e) « ex » sur les réseaux sociaux est une « cyberviolence » devenue un mode de vengeance d'autant plus attentatoire à l'image que la diffusion en cascade est très difficile à maîtriser. Comme cela a été rappelé lors des débats parlementaires, 90% des victimes sont des femmes qui évoquent souvent un viol virtuel.

Le RANSOMHACK : une nouvelle forme de menace de déstabilisation des entreprises

- nouvelle technique d'extorsion apparue depuis l'entrée en vigueur du RGPD.
- repose sur la dénonciation des entreprises victimes de vols de données.
- Elle peut aller jusqu'à la dénonciation de non conformité ou d'entretien de risques élevés sur la confidentialité des données.

Vulnérabilités technologiques: constat

- Les applications vulnérables sont le vecteur le plus fréquemment utilisé pour attaquer des victimes et voler des données personnelles (mots de passe, données bancaires, données personnelles ou même les communications privées des utilisateurs.
- Loi « Business First »

Quelques chiffres

- 76 % des applications iOS et Android présentent des vulnérabilités liées au stockage de données non sécurisées, susceptibles de mettre en danger les données a data des utilisateurs.
- 35 % des applications ne répondent pas à tous les critères de sécurité en matière de transmission des données.
- 89 % des vulnérabilités découvertes peuvent être exploitées via un malware, sans aucune nécessité pour le pirate d'avoir un accès physique à l'appareil de sa victime.
- 20% des applis bancaires mobiles contiennent des failles critiques (92% *contiennent au moins une vulnérabilité de sécurité à risque moyen*) ;
- Le nombre d'alertes de vulnérabilité rapportées par les fournisseurs est en constante augmentation

Faille 0 Day

- Vulnérabilité détectée dans une application ou processus informatique, dont l'éditeur lui-même n'a pas encore connaissance, mais qui est d'ores et déjà exploitée pour pirater des systèmes.
- Elles sont particulièrement précieuses pour les cybercriminels
- Ces vulnérabilités entraînent un délai de réponse fortement accru et offrent plus de temps aux pirates pour s'en servir. En moyenne 59 jours aux éditeurs de logiciels pour créer et déployer des correctifs

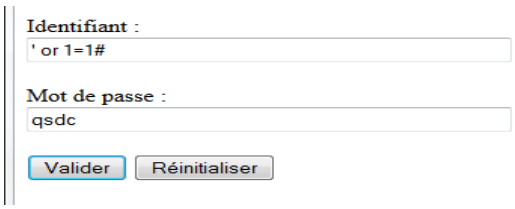
EXPLOIT

- Est un programme qui permet d'exploiter une faille dans un système d'exploitation ou un logiciel
- L'exploit peut-être local ou distant

Il s'agit de proposer une procédure (sous la forme de logiciel) permettant l'exploitation d'une faille d'un logiciel

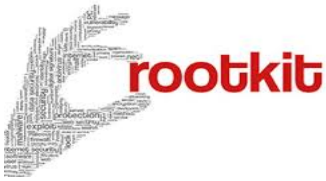
Vulnérabilité des applications
Exemple: INJECTIONS SQL

- Exploitation d'une faille de sécurité (ou vulnérabilité) d'une application qui interagit avec une base de données d'un site (les sites de commerces électroniques par exemple) en injectant une requête SQL non prévue
- Consiste à contourner les contrôles et vérifications permettant d'accéder au site en question. Il est possible, parfois, d'avoir directement accès à l'administration de la base de données et récupérer les logins, les mots de passe , des données sur les membres ou clients qui fréquentent le site, ..)..



Rootkit

- Un programme malveillant (ou ensemble de commandes) visant à compromettre un système informatique afin d'obtenir un accès de type Administrateur (Root).
- le vecteur d'infection le plus courant est l'utilisation d'une vulnérabilité du système d'exploitation ou d'une application fonctionnant sur l'ordinateur(SGBD par exemple).



Défaçement des sites

- Le défaçement (ou défaçage) d'un site consiste à défigurer un site en remplacement de la page d'accueil original par une autre.
- Il s'agit d'une exploitation d'une faille présente soit dans la page d'accueil du site soit dans le système d'exploitation du serveur web

Autres modes opératoires pour les cyberattaques: les Malwares

Malwares = "*malicious*" + "*software*"

89

- Malwares (programmes malveillants): « cancer » de l'univers de la cybercriminalité.
- Ils sont développés dans le but soit de:
  - compromettre le fonctionnement d'un système informatique et engendrer des dégâts dans les systèmes informatiques (destruction des données par exemple)
  - escroquer l'utilisateur du système informatique, ouvrir une pore dérobée à des cybercriminels
  - intercepter des communications ou des flux de données
  - ouvrir une pore dérobée à des cybercriminels
  - prendre le contrôle à distance de l'ordinateur de la victime pour l'intégrer dans un botnet et l'utiliser lors d'une attaque DDoS (Distributed Denial of Service)

Malwares: modes opératoires

Exemples: virus, ver, spyware, troyens (trojans), keyloggers, backdoors, Rootkit, Etc.

- Chaque programme malveillant dispose de propriétés qui lui sont propres.
- les frontières entre chacun d'eux s'amenuisent de plus en plus, à mesure que les cybercriminels conçoivent des codes malveillants combinant plusieurs caractéristiques.
- exploitent les vulnérabilités des applications les plus populaires afin de se propager et de mener des actions néfastes
- Ils sont introduits à l'insu de l'utilisateur par le biais de :
  - pièces jointes ou sous forme d'images dans les messages (exemples: publicité pour des faux-antivirus
  - applications rendant un vrai service sur Smartphone ou un ordinateur

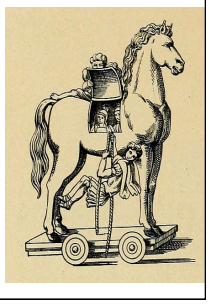
plus d'un tiers des entreprises ont téléchargé un fichier infecté par des logiciels malveillants.

Exemple de malware: Cheval de Troie (troyens - trojans)

- Une des principales menaces sur Internet, le cheval de Troie, comme son nom l'indique, va maquiller sa nature pour s'installer sur un poste.
- Désigne un programme, inoffensif en apparence, qui s'installe de façon frauduleuse (souvent par le biais d'un mail, d'une page web visitée ou d'un programme installé) pour exécuter, à l'insu de l'utilisateur, des opérations malveillantes.
- Contrairement aux Vers ou aux Virus, un Cheval de Troie ne se reproduit pas.

Objectifs: véhiculer des codes malveillants

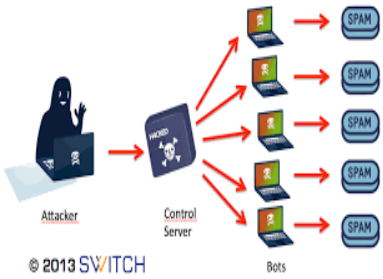
- Prendre le contrôle à distance du système informatique
- Afficher des fausses alertes
- Inciter les utilisateurs à visiter certains sites
- Modifier la page d'accueil d'un site
- Mettre en place une porte dérobée



Botnet et Attaque DDoS
Vers l' industrialisation de la Cyberdélinquance

DDoS (Distributed Denial of Service): attaque informatique ayant pour finalité de rendre indisponible l'accès à un service en le saturant de requêtes.

Botnet: réseau d'ordinateurs corrompus contrôlés par un ou plusieurs cybercriminels pouvant être utilisé pour différentes finalités : émission de spam, diffusion de phishing ou de malware, fraude au clic, attaque DDoS, etc



Loi Godfrain du 5.01.1988 : Sanctions pour atteinte aux STAD

Infractions indispensables pour la lutte contre la cybercriminalité dans l'entreprise

- L'article 323-1 du code pénal sanctionne «le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé». La peine encourue est 2 ans d'emprisonnement et 30000€ d'amende.
- Celle-ci peut être portée à 3 ans d'emprisonnement et 45000€ d'amende lorsqu'il en résulte «soit la suppression, soit la modifications de données contenues dans le système, soit un altération du fonctionnement de ce système».
- Entrave au fonctionnement d'un STAD : 323-2 C. pen.

STAD, Système de traitement automatisé des données

94

- Tout équipement (de nature matérielle, logicielle, ou "firmware") permettant l'acquisition automatique, le stockage, la manipulation, le contrôle, l'affichage, la transmission ou la réception de données.

Ransomware (rançongiciels)

- Les ransomwares constituent la menace principale pour les entreprises et les particuliers.
- Installation de logiciels malveillants qui prennent le contrôle des PC, tablettes et smartphones
- Menace l'utilisateur d'un système informatique de bloquer le système les programmes et/ou chiffrer le contenu des disques.
- Réclamer aux utilisateurs de l'argent pour débloquer leurs machines
- L'utilisation des Ransomwares a augmenté de plus de 93% contre les particuliers et de 90% contre les entreprises. Le mois de septembre 2017 détient le record du plus grand nombre d'attaques au Ransomware contre les entreprises.
- Entre juillet et septembre 2017, on observe une augmentation de 700% de la détection des Ransomwares
- 2019 a bien été l'année du retour en force des ransomwares.

Le rançongiciel est- il saisi par le droit ?

Le rançongiciel est- il saisi par le droit ?

- La réponse est positive
  - C'est un logiciel malveillant, donc répréhensible
    - Notamment l'offre, l'importation, la détention, la mise à disposition ou la cession de programmes malveillants (art. 323-3-1 du Code pénal)
- Il a de nombreuses et importantes conséquences juridiques tant sur le plan matériel qu'immatériel :
  - Perte de données à caractère personnel
  - Atteinte à la sécurité du système d'information Notamment par l'introduction frauduleuse de données

Autres formes de cyberattaques
LE CARDING

- Désigne la création de cartes virtuelles.
- C'est une fraude à la carte bleue.
- Sur certains sites (Darknet), il est possible d'acheter ou de vendre des accès à des comptes bancaires, des numéros de cartes volés, des copies de pistes magnétiques et des profils personnels complets.

Que faire pour une victime (personne qui subit personnellement et directement un préjudice physique, moral ou matériel) ?

- Dépôt de plainte ?
- Dépôt de plainte avec constitution de partie civile ?
- Obligations de notifier les violations de données à caractère personnel
- Obligation de déclarer les incidents de sécurité pour certains types d'acteurs (OIV par exemple)

Fin Partie 2

Merci de votre attention

Adel Jomni