CYBERSECURITÉ

Version TTR

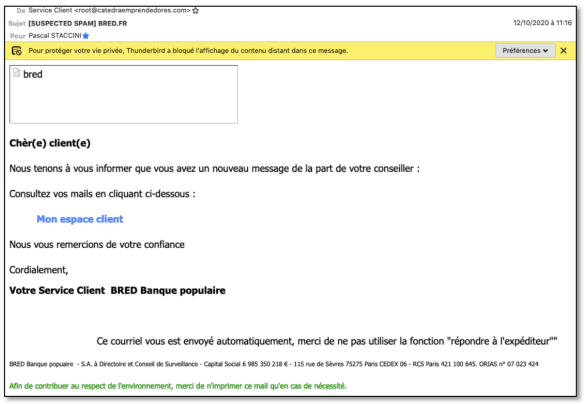
I) Position du problème

A) Cybermenaces

La cybercriminalité	comprend des acteurs isolés ou des groupes qui ciblent des systèmes pour des **gains financiers** ou pour causer des perturbations
Les cyberattaques	impliquent souvent la collecte d'informations pour des raisons **politiques**
Le cyberterrorisme	vise à saper les systèmes électroniques pour entraîner la **panique ou la peur**

B) Typologie des méthodes d'attaque

Malware	Programmes malveillants *(Ce sont des logiciels créés pour faire du mal à ton ordinateur)*
Injection SQL	C'est le fait d'i**nsérer du code malveillant** dans une base de données (ex: formulaire de connexion) **via une déclaration SQL** (SQL = « langage de requêtes structurées ») malveillante. Ils **gagnent ainsi l'accès** à des informations sensibles contenues dans la base. *(en gros le SQL malveillant est un code que le pirate injecte pour tromper le site et accéder à des données qu'il ne devrait pas voir.)*
Attaques par phishing (= tentative d'hameçonnage)	consiste en l'**envoi d'emails** qui semblent provenir d'une entreprise légitime. Ils servent souvent à **tromper les utilisateurs pour récupérer leurs coordonnées** bancaires et d'autres informations personnelles.

	ex:  De BNPPARIBAS-ANTILLES <emails@cloudcone.com> Sujet 01-MESSAGE IMPORTANT Pour Pascal STACCINI ---MESSAGE AUTOMATIQUE--- Cher client, Vous avez reçu un message de sécurité de votre conseiller. IDENTIFIEZ-VOUS βNPPARIβAS-ANTILLES  De Service Client <root@catedraemprendedores.com> Sujet [SUSPECTED SPAM] BRED.FR 12/10/2020 à 11:16 Pour Pascal STACCINI Pour protéger votre vie privée, Thunderbird a bloqué l'affichage du contenu distant dans ce message. Préférences bred Chèr(e) client(e) Nous tenons à vous informer que vous avez un nouveau message de la part de votre conseiller : Consultez vos mails en cliquant ci-dessous : Mon espace client Nous vous remercions de votre confiance Cordialement, Votre Service Client BRED Banque populaire Ce courriel vous est envoyé automatiquement, merci de ne pas utiliser la fonction "répondre à l'expéditeur"" BRED Banque populaire - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 985 350 218 € - 115 rue de Sèvres 75275 Paris CEDEX 06 - RCS Paris 421 100 645. ORIAS n° 07 023 424 Afin de contribuer au respect de l'environnement, merci de n'imprimer ce mail qu'en cas de nécessité.
Attaque dite de l'homme du milieu	Un type de cybermenace consistant à **intercepter la communication** entre deux individus pour leur **voler des données**. Par exemple, sur un réseau wifi non sécurisé, un cybercriminel pourrait intercepter les données transitant entre l'appareil de la victime et le réseau.
Attaque par déni de service	Désigne le fait, pour les cybercriminels, d'**empêcher un système informatique** de répondre à des requêtes légitimes en **surchargeant les réseaux et les serveurs avec du trafic**. Le système devient ainsi inutilisable, empêchant une entreprise de mener à bien l'essentiel de ses tâches.
L'« inside job »	La fuite de données provient d'un des collaborateurs de l'entreprise

C) Nouvelles cybermenaces

Malware Dridex	En décembre 2019, le ministère de la justice américain a poursuivie en justice le chef d'un groupe cybercriminel organisé pour son rôle dans une attaque mondiale. Dridex(= nom du logiciel) est un cheval de Troie bancaire, arrivé en 2014, il infecte les ordinateurs via des emails de phishing ou des malwares existants. Capable de voler les mots de passe, les coordonnées bancaires et les données personnelles qui pourront être utilisés pour effectuer des transactions malhonnêtes, il a causé des pertes financières massives s'élevant à des centaines de millions. En réponse aux attaques Dridex, le National Cyber Security Centre anglais conseille au public de « s'assurer que ses appareils sont patchés, que son antivirus est activé et à jour, et que ses fichiers sont sauvegardés »
Arnaques sentimentales	En février 2020, le FBI mettait en garde les citoyens américains contre les escroqueries mises en place par les cybercriminels sur les sites de rencontre, les salons de discussion et les applications. Leurs auteurs profitent des personnes à la recherche de nouveaux partenaires en les dupant pour obtenir leurs données personnelles. Les arnaques sentimentales ont touché 114 victimes au Nouveau-Mexique en 2019, générant une perte financière d'1,6 million de dollars
Malware Emotet	Fin 2019, l'Australian Cyber Security Center mettait en garde les organisations nationales contre une cybermenace mondiale impliquant le malware Emotet. Emotet est un cheval de Troie sophistiqué capable de voler les données et également de télécharger d'autres malwares. il se propage surtout à cause de mots de passe peu sophistiqués : un rappel de l'importance de créer un mot de passe sûr pour se prémunir contre les cybermenaces.

D) Programme malveillant

= Les **malwares** désignent des **logiciels malveillants**. Il s'agit de l'une des **cybermenaces les plus courantes**, conçue par un **cybercriminel** ou un **hacker** dans le but de **perturber** ou **endommager** l'ordinateur d'un utilisateur. Souvent propagés par des **pièces jointes d'emails indésirables** ou des **téléchargements qui semblent sûrs**, les malwares peuvent être utilisés pour **gagner de l'argent**, ou lors de **cyberattaques à but politique.**

Il existe plusieurs type de malwares : *(définitions ultra importantes +++)*

- **Virus :** un programme pouvant se **dupliquer** qui s'attache à un **fichier sain** et se **propage** dans tout le système en **infectant les fichiers** à l'aide d'un **code malveillant.**
- **Cheval de Troie :** type de programmes malveillants se faisant passer pour **des logiciels authentiques**. Les cybercriminels piègent les utilisateurs en téléchargeant des chevaux de Troie dans leur ordinateur pour **endommager** ou **collecter** des données.
- **Spyware :** un programme **espion** qui enregistre secrètement les **actions d'un utilisateur** au profit des cybercriminels. Par exemple, un spyware peut enregistrer des coordonnées bancaires.
- **Ransomware :** un malware qui **verrouille les fichiers** et les **données** de l'utilisateur sous menace de les effacer si une **rançon** n'est pas payée.
- **Adware :** un logiciel **publicitaire** qui peut être utilisé pour propager un malware
- **Botnets :** des réseaux **d'ordinateurs infectés** par des malwares que les cybercriminels peuvent utiliser **pour effectuer des tâches en ligne sans l'autorisation** de l'utilisateur.

E) Fuite de données

Une **fuite de données** = une **exposition non désirée**, qu'elle soit **publique ou privée**, touchant une **entreprise** ou un **particulier**.

Les **principales causes** sont :

- les **cyberattaques** (**48 %**),
- l'**erreur humaine** (**27 %**),
- l'**erreur système** (problèmes IT ou internes) (**25 %**).

Au **premier semestre 2019**, la France a enregistré en moyenne **5,7 violations de données**
par jour, contre **4,5 au deuxième semestre 2018.**

Dans **54 %** des cas, ces fuites étaient **d'origine malveillante**, principalement dues à :

- du piratage en ligne (69,8 %)
- et du vol physique (15 %). *Par ex : vol clés USA, telephones…etc*

Environ **26 %** des fuites sont **accidentelles**, et le reste est dû à des causes **inconnues** ou classées comme **autres**.

Le **secteur le plus touché** est celui des **sciences et techniques** 🧪 avec 297 notifications entre juin 2018 et juin 2019.
Viennent ensuite :

- le **commerce** 🛒 (**279 violations**),
- la **finance** 💰 (**275**),

- l'**administration publique** 🏛️ (**229**),
- et enfin l'**hébergement et la restauration** 🍽️ (**202 notifications**).

Pour un attaquant, le vol de données permet :

- De **financiariser une arnaque** : en vendant les données collectées ;
- De **compléter une attaque** : le vol de données permet d'acquérir ou d'amasser de la connaissance sur une cible précise, avant de lancer ensuite une attaque de plus grande Importance.

Exemple :

En 2018, le scandale Facebook-Cambridge Analytica : fuite des données personnelles de 87 millions d'utilisateurs Facebook que la société Cambridge Analytica (CA) a commencé à recueillir dès 2014. Les informations ont été obtenues par l'application « thisisyourdigitallife », un test de personnalité monté par l'universitaire Aleksandr Kogan de Cambridge, via sa société Global Science Research (GSR). Par ce biais, les internautes autorisaient à la fois la captation de certaines de leurs données (comme la ville ou les contenus aimés) mais aussi certaines infos de leurs amis, si leurs paramètres les permettaient. Ces informations ont servi à influencer les intentions de vote en faveur d'hommes politiques qui ont retenu les services de CA. L'affaire Cambridge Analytica a valu au réseau social une amende record de 5 milliards de dollars, infligée par la FCC, la Commission fédérale des communications américaines.

Toutes **régions du monde confondues**, il faut en moyenne **197 jours** à une **entreprise** pour **découvrir** qu'une **fuite de données** (ou **data breach**) a eu lieu.
Une fois la brèche identifiée, le **temps moyen de résolution** est de **69 jours**.

🛡️ Les **facteurs qui réduisent l'impact** d'une fuite de données sont :

- l'**implication du comité de direction** dans les questions de **cybersécurité**,
- la **sensibilisation des employés**,
- la **classification des données** selon leur niveau de sensibilité,
- l'utilisation d'un **logiciel de Data Loss Protection (DLP =** logiciel de protection des donnée**)**
- la présence d'une **équipe de réponse aux incidents** (interne ou externe) en cas de brèche.

Conduite à adopter en cas d'incident de cybersécurité

- **Prévenir** : préparer à l'avance les équipes **techniques** et **non techniques** à la gestion d'une éventuelle attaque.
- **Détecter** : mettre en place une **équipe de cyber intelligence** pour identifier rapidement les menaces.
- **Assurer** : disposer d'une **couverture adaptée** pour prendre en charge les conséquences (frais de gestion, notifications obligatoires, pertes financières, etc.).
- **Réagir** : **notifier la CNIL dans un délai de 72 heures** après la découverte de l'incident.

II) Sécurité informatique

A) Définition de la cybersécurité

- La **cybersécurité** permet de gérer les **données** dans des conditions **optimales** et **sécurisées**.
- Elle consiste à **protéger** les **ordinateurs**, **serveurs**, **appareils mobiles**, **systèmes électroniques**, **réseaux** et **données** contre les **attaques malveillantes**.
- On parle aussi de **sécurité informatique** ou de **sécurité des systèmes d'information**.

Elle concerne de nombreux domaines : de **l'informatique d'entreprise** aux **terminaux mobiles**… même le **secteur de la santé** est concerné !

B) Objectifs de la cybersécurité

- **L'intégrité** : garantir que les **données** n'ont pas été altérées et sont bien celles que l'on croit être.
- **La confidentialité** : veiller à ce que **seules les personnes autorisées** puissent accéder aux ressources ou informations échangées.
- **La disponibilité** : s'assurer que le **système d'information reste accessible** et fonctionne correctement en toute circonstance.
- **La non-répudiation** : garantir qu'une **action ou transaction ne puisse être niée**
- **L'authentification** : permettre de **vérifier l'identité** des utilisateurs afin que seuls les **accès autorisés** soient accordés.

C) Sécurité physique

La **sécurité physique** vise à **contrôler l'accès** aux locaux, ordinateurs et équipements grâce à des dispositifs concrets : **barrières**, **alarmes**, **serrures**, et autres **mécanismes de contrôle d'accès**.

Ces mesures sont essentielles pour **protéger les matériels** (ordinateurs, serveurs, câbles, etc.) et leur contenu contre : **le vol**, **l'espionnage**, **la destruction accidentelle ou intentionnelle**

Risques physiques à prendre en compte :

- **Dégâts des eaux**
- **Problèmes électriques**
- **Défaillance de la climatisation**
- **Incendies**
- **Électricité statique**
- **Intervention physique non autorisée**
- **Perturbations liées aux réseaux de communication**
- **Accès non sécurisé à la salle informatique**

D) Sécurité logique

La **sécurité logique** repose sur la mise en œuvre d'un **système de contrôle d'accès logique** s'appuyant sur un service d'**authentification**, d'**identification** et d'**autorisation**, et elle repose également sur : les dispositifs mis en place pour garantir la **confidentialité** dont la **cryptographie**, une gestion efficace des **mots de passe** et des **procédures d'authentification**, des mesures **antivirus** et de **sauvegarde** des informations sensibles.
Elle comprend également des dispositifs garantissant la **confidentialité des données**, comme la **cryptographie**, une bonne **gestion des mots de passe**, des **procédures d'authentification solides**, des **solutions antivirus** fiables, et des **systèmes de sauvegarde** pour les données sensibles.

🎯 Objectifs :

- **Confidentialité des accès**
  → pour prévenir l'**usurpation d'identité** et le **vol d'informations critiques**
- **Disponibilité des ressources**
  → pour éviter les **arrêts de production** ou pannes imprévues
- **Intégrité des données**
  → pour protéger la **qualité des informations** et préserver **l'image de l'organisation**

🛠️ Mécanismes utilisés dans les logiciels de sécurité

- **Contrôle d'accès logique** :
  ➤ Identification, authentification, autorisation

- **Protection des données** :
  ➢ Cryptage, antivirus, sauvegarde régulière

E) Typologie des sécurités

La sécurité des réseaux	protège le **réseau informatique** contre les **intrusions**, qu'il s'agisse d'**attaques ciblées** ou de **malwares opportunistes**
La sécurité des applications	protège les **logiciels** et **appareils** contre les **menaces**. Une application corrompue peut compromettre l'accès aux **données**. Une **sécurité fiable** se reconnaît dès la **conception**, avant le déploiement d'un programme ou appareil.
Le sécurité des informations	garantit l'**intégrité** et la **confidentialité** des **données**, stockées ou en transit.
Le sécurité opérationnelle	englobe les **processus** et **décisions** liés au traitement et à la protection des données, notamment les **autorisations d'accès** et les procédures de **stockage** et de localisation des données
La reprise après sinistre et la continuité des opérations	définissent la réponse d'une entreprise face à un **incident de cybersécurité** ou à une perte d'**opérations** ou de **données**. Les politiques de reprise encadrent la restauration des **opérations** et des **informations** pour retrouver la capacité d'avant l'événement. La continuité des opérations décrit le plan permettant de fonctionner malgré l'absence de certaines **ressources**.
La formation des utilisateurs finaux	cible le facteur le plus **imprévisible** : les **personnes**. Elles peuvent involontairement introduire des **virus** en ne suivant pas les bonnes pratiques. Former les utilisateurs à éviter les **pièces jointes suspectes** et les **clés USB non identifiées** est crucial pour la **sécurité** de l'entreprise.

F) Classes des cybersécurités

Classe 1
Il s'agit des **systèmes industriels** pour lesquels le **risque** ou l'**impact** d'une attaque est **faible**. L'ensemble des **mesures préconisées** pour cette classe doivent pouvoir être appliquées en **complète autonomie**. Ce niveau correspond principalement aux **règles d'hygiène informatique** énoncées dans le **guide de l'ANSSI**.

Classe 2
Il s'agit des **systèmes industriels** pour lesquels le **risque** ou l'**impact** d'une attaque est **significatif**. Il n'y a pas de **contrôle étatique** pour cette classe de système industriel mais l'**entité responsable** doit pouvoir apporter la **preuve** de la mise en place des **mesures adéquates** en cas de **contrôle** ou d'**incident**.

Classe 3
Il s'agit des **systèmes industriels** pour lesquels le **risque** ou l'**impact** d'une attaque est **critique**. Dans cette classe, les **obligations** sont plus fortes et la **conformité** de ces systèmes industriels est vérifiée par l'**autorité étatique** ou un **organisme accrédité**.

FIN

Voilà, c'est la fin du cours version TTR. Je sais que la SN, c'est vraiment pas fun, voire même relou à réviser et parfois difficile à comprendre, mais en vrai les cours ne sont pas si longs. Lisez-les pendant les moments où vous avez un petit coup de fatigue, et vous verrez. Ce sont des QRU : avoir vu le cours au moins une fois, par élimination, vous pouvez avoir tous les points.