



# La Cybersécurité: Présentation globale

SIO - Bloc 1 - SMDSI

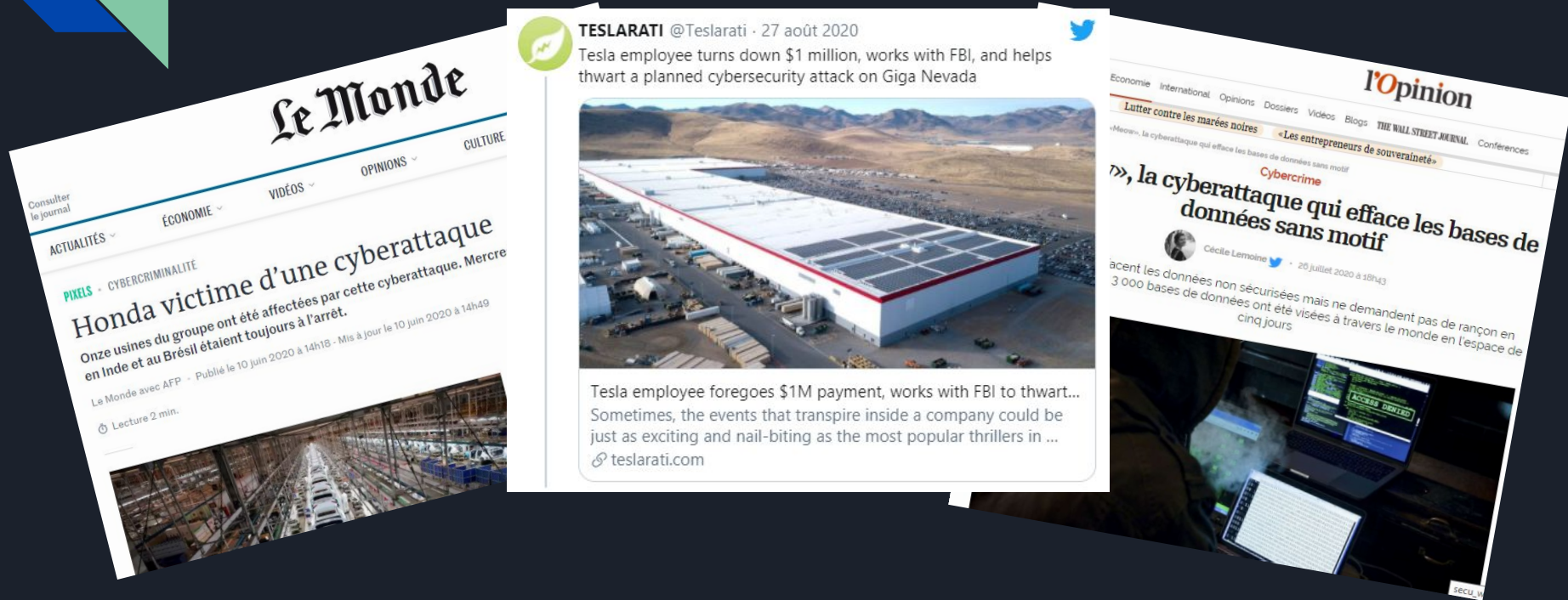
M. SPINA



# Sommaire

1. Introduction
  - a. Etat des lieux des réseaux d'entreprise
  - b. Illustration en chiffres
2. Qu'est-ce que la cybersécurité ?
3. Au sein du BTS SIO
4. Les missions de la cybersécurité
  - a. Les niveaux de sécurité

# Introduction



Vu dans la presse et sur les réseaux sociaux


# Introduction



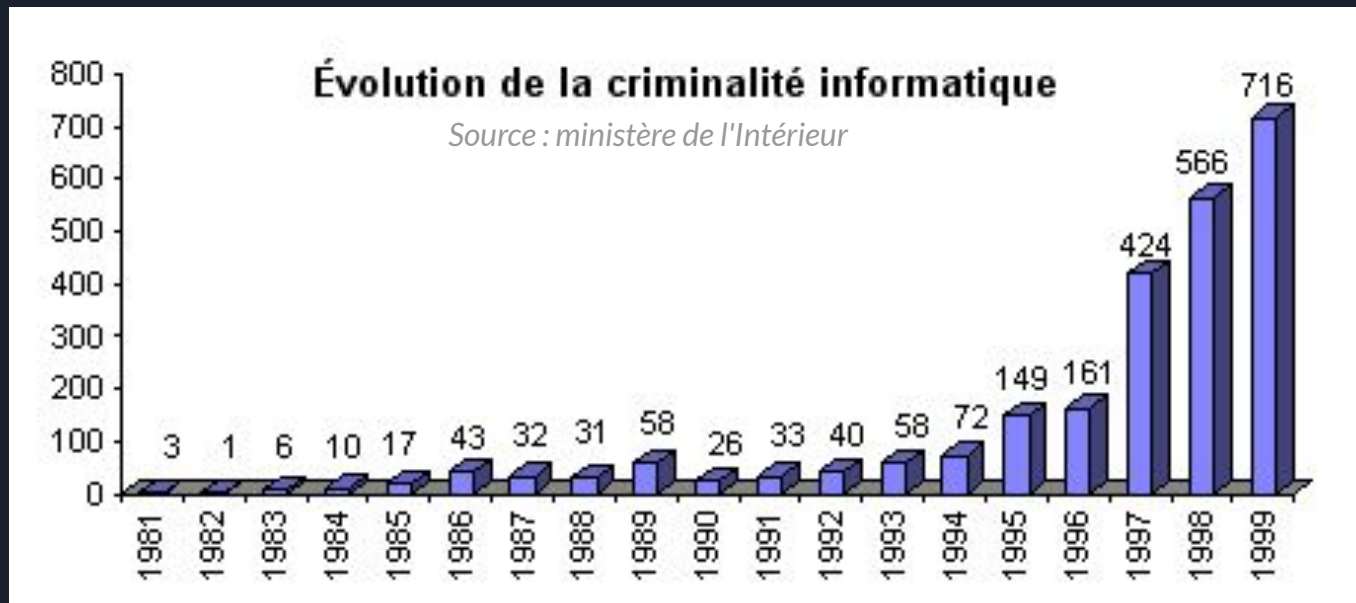
Vu dans les films et les séries



# Etat des lieux sur les réseaux d'entreprise:

HIER	AUJOURD'HUI
centralisé: localement échanges papier pas d'accès distants	distribué sur plusieurs sites accès distants multiplication des sous-traitants
<b>Conséquences:</b> <ul style="list-style-type: none"><li>- augmentation des communications et de la mobilité</li><li>- dépendance au système informatique</li></ul>  <b>moins de contrôle de l'information &amp; augmentation des risques diverses</b>	

## Illustration en chiffres:





# Qu'est-ce que la cybersécurité ?

La cybersécurité consiste à **assurer** que les ressources numériques d'une entité, qu'elles soient :

- matérielles (ex : ordinateur, serveur, robot, imprimantes, appareils mobiles),
- logicielles (ex : programmes et données personnelles),
- ou de communication (ex : réseau local, internet, messagerie),

sont **protégées contre toute attaque malveillante**, qui les détournerait de leur fonctionnement initialement prévu.



# Qu'est-ce que la cybersécurité ?

On l'appelle également sécurité informatique ou sécurité des systèmes d'information.

Aujourd'hui, tout le monde peut être victime d'une attaque, un réseau d'entreprise ou même un simple terminal mobile.

Il existe énormément de types d'attaques différents, c'est pourquoi la cybersécurité s'applique sur plusieurs niveaux.





# Au sein du BTS SIO

## **Cybersécurité des services informatiques**

*Protection des données à caractère personnel*

*Préservation de l'identité numérique de l'organisation*

*Sécurisation des équipements et des usages des utilisateurs*

*Garantie de la disponibilité, de l'intégrité et de la confidentialité  
des services informatiques et des données de l'organisation face  
à des cyberattaques*



# Au sein du BTS SIO

## **Cybersécurité des services informatiques**

*Protection des données à caractère personnel*

*Préservation de l'identité numérique de l'organisation*

*Sécurisation des équipements et des usages des utilisateurs*

*Garantie de la disponibilité, de l'intégrité et de la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques*

### **Option SISR**

*Cybersécurisation d'une infrastructure réseau, d'un système, d'un service*

### **Option SLAM**

*Cybersécurisation d'une solution applicative et de son développement*



# Au sein du BTS SIO

## **B3-1. Protection des données à caractère personnel**

- Recensement des traitements sur les données à caractère personnel au sein de l'organisation
- Identification des risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel
- Application de la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel
- Sensibilisation des utilisateurs à la protection des données à caractère personnel

.....



# Les missions de la cybersécurité

Celle-ci vise à garantir:

- **la disponibilité** des ressources numériques (ex : avoir accès à sa machine ou aux informations à tout moment, y compris en cas d'attaques)
- **l'intégrité**, c'est-à-dire la conformité des ressources numériques (ex : la machine réalise l'action demandée et uniquement celle-là, les informations sont toujours entières et correctes)
- **la confidentialité** des ressources numériques (ex : les données clients ne doivent pas être rendues accessibles, limitation des droits d'accès)
- **la preuve**, c'est-à-dire la traçabilité de l'information (ex: surveillance du réseau)



# Les niveaux de sécurité

La **sécurité des réseaux** consiste à protéger le réseau informatique contre les intrus, qu'il s'agisse d'attaques ciblées ou de malwares opportunistes.

La **sécurité des applications** vise à protéger les logiciels et les appareils contre les menaces. Une application corrompue pourrait ouvrir l'accès aux données qu'elle est censée protéger.

La **sécurité des informations** veille à garantir l'intégrité et la confidentialité des données, qu'elles soient stockées ou en transfert.



# Les niveaux de sécurité

La **sécurité opérationnelle** comprend les processus et les décisions liés au traitement et à la protection des données. Ce niveau de sécurité permet de définir les autorisations des utilisateurs pour l'accès au réseau, les procédures qui attribuent l'espace de stockage et l'emplacement des données

La **continuité des opérations (ou reprise après sinistre)** spécifient la manière dont une entreprise répond à un incident de cybersécurité causant une perte des opérations ou de données. La continuité des opérations se réfère au plan qu'a mis en place une entreprise qui permet de fonctionner sans certaines ressources.



# Questions



?