CPNE centre de formation professionnelle neuchâtelois

# INTRODUCTION À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

## Sécurité

## INT_TEC1_SEC

LJA

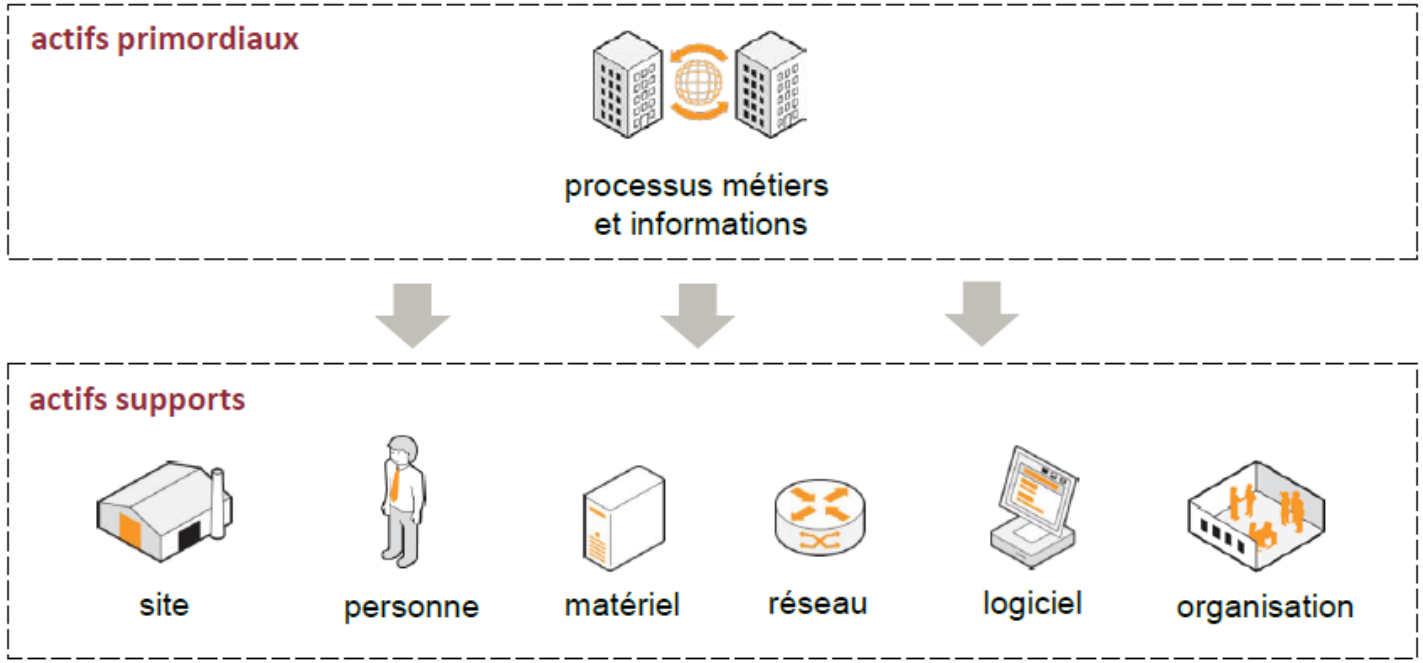
Janvier 2024

# Système d'information

## DÉFINITION

Système d'information (SI): Ensemble de ressources (actifs ou assets) destinées à collecter, classifier, stocker, gérer diffuser les informations au sein d'une organisation

Le SI doit permettre et faciliter la mission de l'entreprise.



# Les enjeux de la cybersécurité

«LA QUESTION N'EST PLUS DE SAVOIR SI, MAIS QUAND VOUS SEREZ HACKÉ»

La cybersécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers d'une entreprise ou collectivité

La cybersécurité ne devrait ***pas être contraignante*** pour l'utilisation d'un système d'information. Elle contribue à la qualité et la protection du service de ce dernier. → Illustration en image

Contribution à la qualité de service et à un niveau de protection attendue par les utilisateurs (clients, employées, fournisseurs, etc).

# Les enjeux

**À savoir**

Parmi les 347 000 cyberattaques réussies touchant des entreprises en 2022, 330 000 concernent les PME[2]. Un chiffre d'autant plus préoccupant que **60 % des PME victimes d'une cyberattaque font faillite dans les 18 mois**[3].

## IMPACTS

- Financiers
- Juridiques et réglementaires
- Dégâts de réputation
- Organisationnels

# Sécurité globale

## LA SURETÉ

**La sureté:** protection contre le dysfonctionnements et accidents involontaire. Quantifiable statistiquement

- Sauvegarde
  - Incendie du datacenter SGB2 chez OVH
- Redondance
  - Fermeture de l'espace aérien suisse pendant deux heures
- Dimensionnement de l'infrastructure

## LA SÉCURITÉ

**Sécurité:** protection contre les actions malveillantes volontaires

- Déni de service
  - DDOS sur l'administration fédérale durant le WEF
- Vol de données ou destruction de données
  - Vol de données chez Dataport
- Cryptage ou divulgation de données
  - Données classifiées de la confédération sur le darknet suite à l'attaque contre XPLAIN

# Objectifs de la sécurité

LES QUATRE CRITÈRES PRINCIPAUX (DIC)

- Disponibilité (D) – capacité d'une ressource à être accessible
- Intégrité (I) – une ressource (donnée) est intacte et complète. Elle n'a pas détruite ou altérée
- Confidentialité (C) – une ressource doit rester secret. Elle accessible uniquement aux personnes autorisées
- La Preuve (P) – fournir une journalisation sur les événements d'un actif. Cela englobe la traçabilité, l'authentification et l'imputabilité

# Attaquants: Acte isolé à organisation criminelles

DE L'EXPLOIT TECHNIQUE AU PIRATAGE D'OPPORTUNITÉ JUSQU'À LA CYBERGUERRE

Année 80 début de l'internet → Bidouilleurs – Hacker isolé – Script-Kiddies (lamer)

Personnel interne

Concurrents – Espionnage industrielle

Organisations criminelles

Hacktiviste

Etat tiers

# Vulnérabilité

## DÉFINITION

Faiblesse ou faille au niveau d'un actif. Elles peuvent être présentes au niveau:

- **De la conception**
- **De la réalisation**
- **De l'installation**
- **De la configuration**
- **De l'utilisation**

## RÉFÉRENCEMENT

- Les vulnérabilités sont référencées par MITRE
- Elle se voit attribué un ID CVE (Vulnerabilities and Exposures)
- ID CVE (*CVE-AAAA-NNNN)*
- https://www.cve.org/

# MENACE

## DÉFINITION

Une menace est quelqu'un ou quelque chose qui peut exploiter une vulnérabilité pour obtenir, modifier ou empêcher l'accès à un système d'information.

Les menaces diffèrent pour chaque entreprise. De plus, elles sont appelées à évoluer dans le temps

## PANORAMA DE MENACES

SPAM – ingénierie sociale – Phising

Fraude interne

Violation d'accès non autorisé

Logiciel malveillant (virus, rootkit, vers, trojan, backdoor)

Déni de service distribué

Ransomware – destruction ou divulgation de données

# Catégorisation des menaces

La base de la pyramide représente un grand nombre d'attaque sans cible précise qui demande peu de moyen. Les dommages sont relativement faibles

Au sommet, il s'agit d'attaques très évolués avec une cible précise. Elles nécessitent des moyens techniques et des compétences élevées. Ces attaques durent dans le temps. Un exemple célèbre est stuxnet