AMINE BENTERKI, YACINE OUISSA

2024

FORMATION À LA CYBERSÉCURITÉ

1. COMPRENDRE LES PRINCIPES FONDAMENTAUX DE LA CYBERSÉCURITÉ

2. IDENTIFIER LES TYPES DE MENACES ET LES VULNÉRABILITÉS COURANTES

3. APPRENDRE LES MÉTHODES DE PRÉVENTION CONTRE LES CYBERATTAQUES

4. SAVOIR COMMENT RÉAGIR EN CAS DE VIOLATION DE LA SÉCURITÉ

LA CYBERSÉCURITÉ, QU'EST-CE QUE C'EST ?

D'un point de vue sémantique :

- cyber, du grec "kybernetes" (pilote, gouvernail)
  contexte moderne : informatique, réseaux numériques

- sécurité :
  sens : protection contre dangers, dommages, pertes

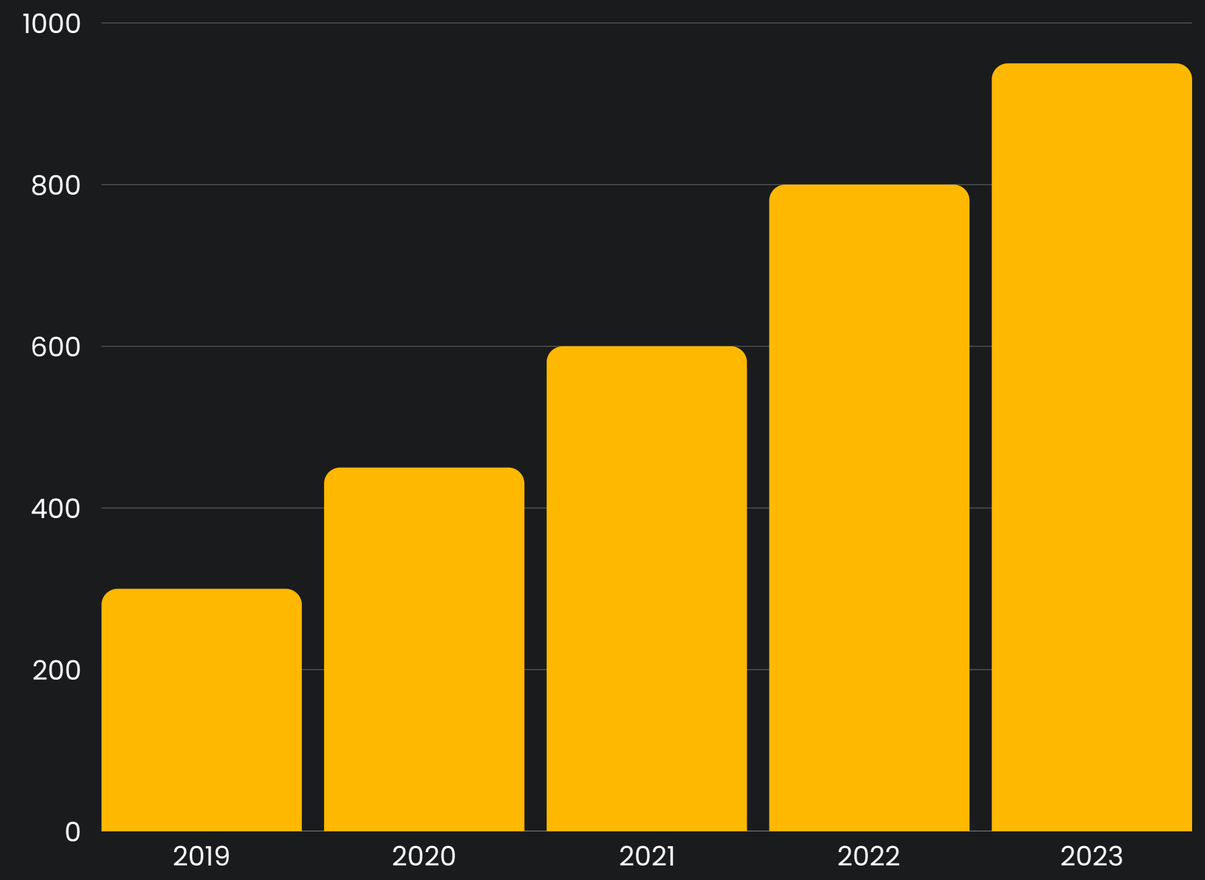
- cybersécurité :
  protection des systèmes et des informations numériques

se protéger contre quoi, contre qui ?

contre les cyberattaques

ÉVOLUTION DES CYBERATTAQUES CONTRE LES ÉTABLISSEMENTS DE SANTÉ

Depuis quelques années, le nombre de cyberattaques visant les établissements de santé a connu une augmentation significative dans le monde



LES PRINCIPALES MENACES EN CYBERSÉCURITÉ

LOGICIELS MALVEILLANTS → VIRUS, CHEVAUX DE TROIE, RANSOMWARES

PHISHING → EMAILS FRAUDULEUX VISANT À OBTENIR DES INFORMATIONS SENSIBLES

ATTAQUES DDOS → SATURATION DU RÉSEAU POUR LE RENDRE INDISPONIBLE

MENACES INTERNES → NÉGLIGENCE OU MALVEILLANCE DES EMPLOYÉS

MESURES DE SÉCURITÉ À METTRE EN PLACE

La CNIL (organisme chargé de protéger les données en France) préconise :

- Utilisation de mots de passe forts : Combinaisons complexes, gestionnaires de mots de passe
- Mises à jour régulières : Systèmes d'exploitation, logiciels
- Sensibilisation au phishing : Reconnaître et signaler les mails frauduleux
- Utilisation de VPN : Sécurisation des connexions à distance
- Sauvegardes régulières : Prévenir la perte de données

EXEMPLE

2024

Etude de cas : Attaque à l'Hôpital

Exemple récent d'attaque cybernétique contre le centre hospitalier sud francilien à Corbeil-Essonnes (2022)

Centre Hospitalier Sud Francilien

- **Symptômes initiaux : Dysfonctionnement informatique**
- **Mesures d'urgences : Isolation des postes infectés, renforcement des contrôles**
- **Conséquences : Perturbation des services, impact sur les patients et le personnel**

PROTOCOLES DE SÉCURITÉ EN ENTREPRISE

- SSL/TLS : Sécurtisation des communications en ligne
- VPN : Sécurisation des connexions à distance
- Pare-feu : Filtrage du trafic réseau
- Antivirus et antimalware : Protection contre les logiciels malveillants
- IDS/IPS : Système de détection et de prévention d'intrusion

EN CONCLUSION

La cybersécurité est une responsabilité partagée. En suivant les meilleures pratiques et en restant vigilant, nous pouvons protéger notre entreprise contre les cybermenaces

MERCI !

Avez-vous des questions ?