Introduction à la Cybersécurité

Dr Yannick BARDIE
President ANAT

Objectifs :

- Comprendre l’importance de la cybersécurité en recherche clinique.
- Identifier les menaces spécifiques aux systèmes d’information dans la santé.
- Découvrir des pratiques clés pour protéger les données sensibles.

Pourquoi la cybersécurité en recherche clinique ?

Enjeux :

- Confidentialité des données des patients.
- Conformité avec les réglementations (RGPD, lois nationales).
- Prévention des cyberattaques (vol de données, *ransomware*).

Impact des failles :

- Perte de confiance des patients.
- Risques légaux et financiers pour les institutions.

Menaces principales

Phishing : Courriels frauduleux visant à voler des identifiants.

Ransomware : Verrouillage des données en échange d'une rançon.

Accès non autorisé : Exploitation de mots de passe faibles ou volés.

Fuites accidentelles : Erreurs humaines dans le partage ou la gestion des données.

Cas concrets dans la santé

Attaques récentes contre des hôpitaux et des instituts de recherche.

Vol de données cliniques sensibles (informations médicales, protocoles d’essai).

Exemples d’impacts financiers et réputationnels.

1. Centre Hospitalier Sud Francilien (CHSF) - Corbeil-Essonnes (Août 2022)

Nature de l'attaque : Rançongiciel (*ransomware*) LockBit.

Conséquences :

- Paralysie totale du système informatique, empêchant l'accès aux dossiers des patients.
- Retour temporaire au papier pour les opérations médicales et administratives.
- Report des consultations non urgentes.
- Fuite de données sensibles (patients, personnel).

Demande de rançon : 10 millions de dollars (refusée par l'hôpital).

Coût estimé :

- **Plusieurs millions d'euros pour la restauration des systèmes informatiques et la gestion de crise.**
- Dépenses en cybersécurité renforcée.

2. Hôpital de Dax (Février 2021)

Nature de l'attaque : Rançongiciel.

Conséquences :

- Blocage de l’ensemble des systèmes informatiques.
- Impossibilité d’émettre des prescriptions, de planifier des interventions ou d'accéder aux dossiers patients.
- Annulation ou report de nombreuses consultations et opérations.

Coût estimé :

- 1,7 million d'euros pour la remise en état des systèmes.
- Impact indirect sur la prise en charge des patients.

3. Centre Hospitalier de Villefranche-sur-Saône et Nord-Ouest (Février 2021)

Nature de l'attaque : Rançongiciel.

Conséquences :

- Blocage des systèmes de gestion hospitalière.
- Perturbations dans la prise en charge des patients.
- Utilisation du papier pour les dossiers médicaux.

Coût estimé :

- Plus de 500 000 euros pour le rétablissement des systèmes.
- Dépenses accrues pour renforcer les infrastructures informatiques.

4. Hôpital de Corbeil-Essonnes (2022)

Nature de l'attaque : Cyberattaque liée à un ransomware.

Conséquences :

- Fuites de données de santé, dont celles des patients.
- Mise hors ligne des systèmes critiques pendant plusieurs semaines.

Coût estimé :

- Plusieurs millions d’euros pour la reconstruction des systèmes.
- Perte de confiance des patients et renforcement de la cybersécurité.

5. Hôpital de Narbonne (Décembre 2020)

Nature de l'attaque : Hameçonnage (*phishing*).

Conséquences :

- Intrusion dans les systèmes via des courriels frauduleux.
- Extraction de données sensibles concernant les patients.

Coût estimé :

- Montants non divulgués, mais les impacts ont engendré des dépenses importantes en sécurisation et audits.

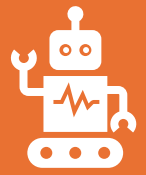
Tendances générales

Augmentation des attaques : Selon l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information), les cyberattaques ciblant les hôpitaux français ont augmenté de 255 % entre 2020 et 2022.

Cibles principales : Les établissements de santé sont souvent considérés comme des cibles faciles en raison de leurs systèmes parfois obsolètes.

Coût moyen par incident : Estimé entre 1 et 3 millions d'euros, en incluant la restauration des systèmes, les audits de sécurité et les pertes d'exploitation.

Solutions mises en place



Renforcement des infrastructures : Déploiement de systèmes informatiques plus résilients.

Formation du personnel : Sensibilisation aux cyberrisques, notamment au hameçonnage.

Collaboration avec l’ANSSI : Pour auditer et sécuriser les systèmes critiques.

Réglementations et cadre légal
RGPD :

- Gestion des données personnelles des patients.
- Droits des patients sur leurs données.

- **Normes spécifiques :**
  - **ISO 27001 pour la gestion de la sécurité de l’information tirée de ISO 31000 (HRO).**
  - Règlementation nationale sur les essais cliniques.

Les bases de la cybersécurité

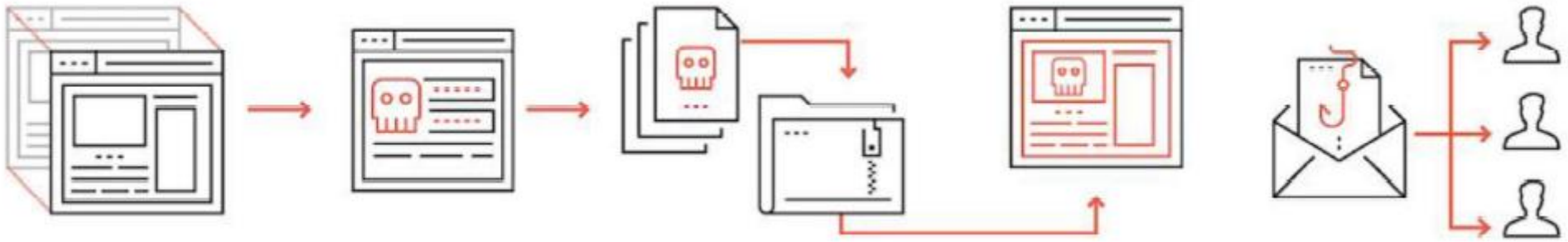
- **Bonnes pratiques individuelles :**
  - Mots de passe robustes et gestionnaire de mots de passe.
  - Méfiance face aux emails suspects.
  - Double authentification.
- **Bonnes pratiques organisationnelles :**
  - Formation régulière des employés (hygiène informatique).
  - Mise à jour des logiciels et des systèmes.
  - Plans de réponse aux incidents.

Spam !

90 % de la correpondante e.mail planétaire est du SPAM !

Arpagian Nicolas, La Cybersécurité, Ed. Que sais-je-PUF

Attaque Type



1.
The legitimate website is cloned

2.
The login page is changed to point to a credential-stealing script

3.
The modified files are bundled into a zip file to make a phishing kit

4.
The phishing kit is uploaded to the hacked website, files are unzipped

5.
Emails are sent with links pointing to the new spoofed website

Outils essentiels

LOGICIELS ANTIVIRUS ET ANTI-MALWARE.

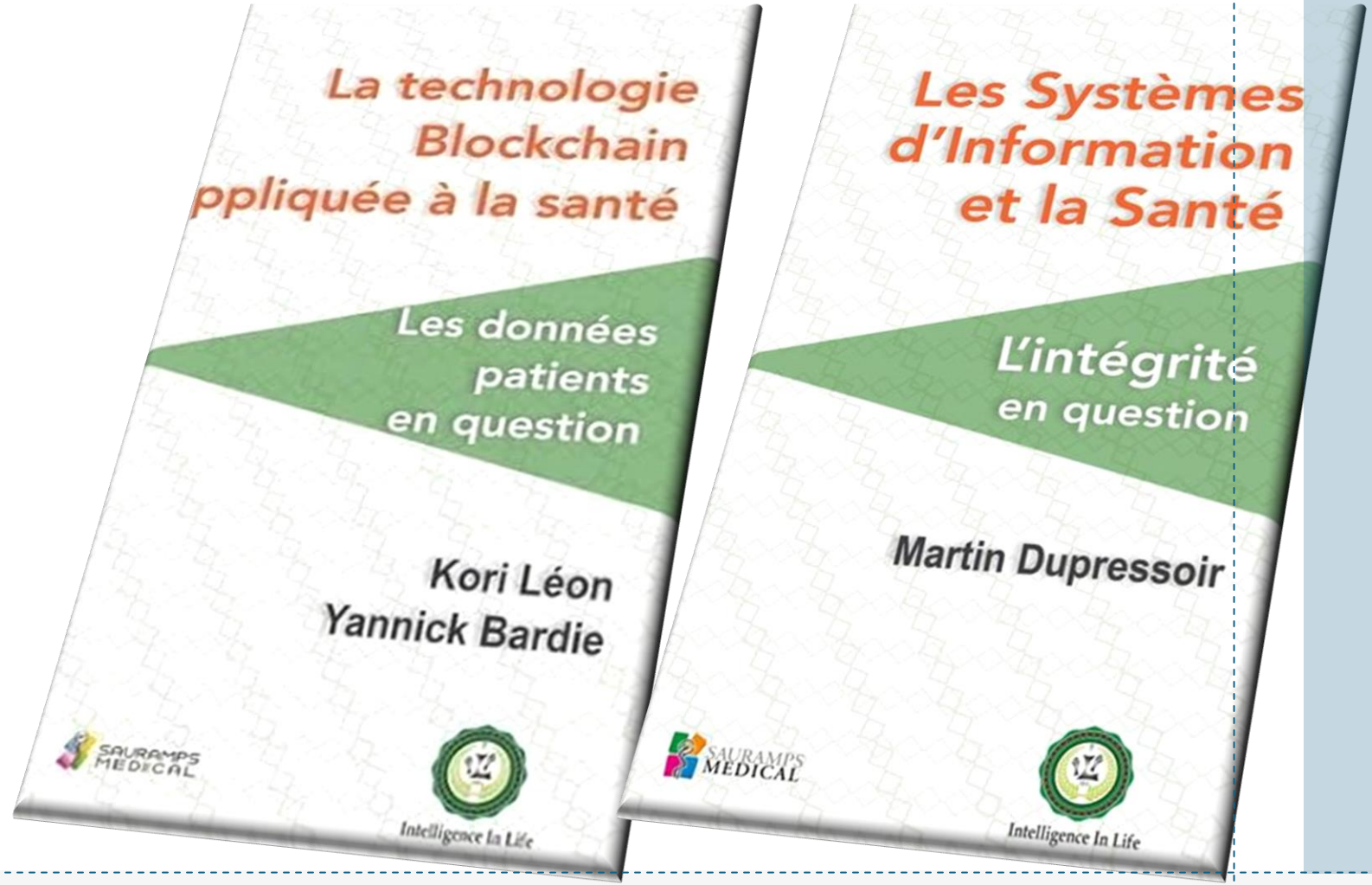
OUTILS DE CHIFFREMENT DES DONNÉES SENSIBLES.

SYSTÈMES D’AUTHENTIFICATION FORTE.

Conclusion et recommandations Synthèse :

La cybersécurité est une responsabilité partagée.

Importance de la vigilance quotidienne et des formations régulières.



Prochaines étapes :

Audit de sécurité de votre organisation.

Mise en place d’une politique de cybersécurité adaptée.

Introduction à la Cybersécurité

Dr Yannick BARDIE
President ANAT