ONE FIRM, MULTIPLE TALENTS

Domaine médical

Cyber-risques et enjeux juridiques

Me Grégoire Chappuis, avocat au barreau de Genève

Introduction

WarGame, 1983

- **Révolution digitale** du domaine de la santé
  - Gestion des dossiers de manière électronique
  - Dossier électronique du patient: introduction progressive
  - Interconnexion des systèmes d'information
- **Avantages vs cyber-risques importants**

Le Bureau des légendes, Saison 5

Plan

1. Cyber-risque : exemple du rançongiciel
2. Enjeux concrets pour le médecin et le patient
3. Obligation légale d'annoncer les failles de sécurité
4. Risques juridiques du médecin

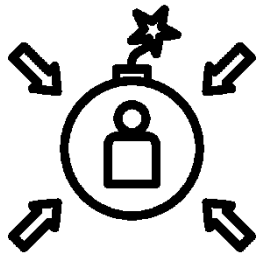
1. Cyber-risque : cas du rançongiciel

- Cyber-risque le plus emblématique : ***ransomware***
- Depuis 2016: **forte croissance** des attaques à l'encontre de PME suisses actives dans le domaine de la santé
- **Forte valeur marchande** des données de santé sur le dark web
- **Victimes**: centres hospitaliers, cabinets, médecins individuels, centres de facturation

1. Cyber-risque : cas du rançongiciel

- Rançongiciel = **logiciel malveillant** infectant les fichiers et systèmes informatiques
- **Moyens** : clé USB, pièce jointe à un e-mail, hyperlien menant à un site malveillant, etc.
- **Cryptage** des données et des systèmes informatiques
- **Rançon** en échange du décryptage (généralement bitcoins)

1. Cyber-risque : cas du rançongiciel



- Moyens des hackers pour **faire monter la pression**:
  - Suppression des sauvegardes
  - Exfiltration des données de patients
  - Publication ou vente des données sur le dark web
- Possible **extorsion subséquente** dirigée contre les patients

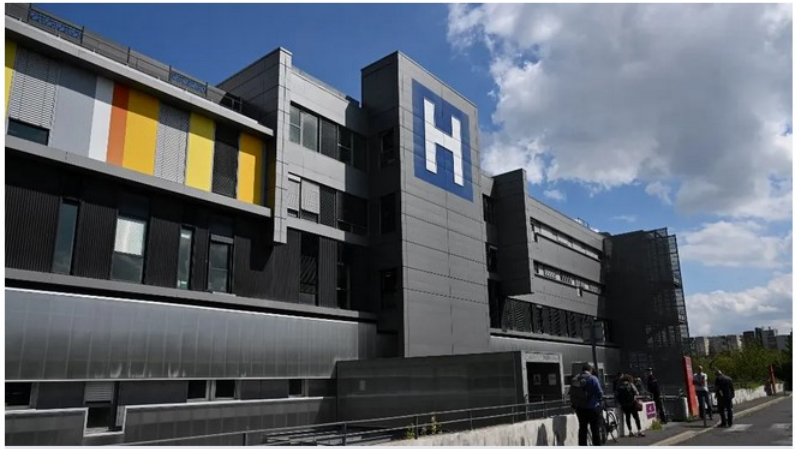
1. Cyber-risque : cas du rançongiciel

Cyberattaque d'un hôpital en Essonne : cinq questions sur les données de santé divulguées

Un groupe de hackers a commencé à diffuser des données piratées lors d'une cyberattaque menée le 22 août. Près de 1,5 million de personnes, patients ou agents de l'hôpital, sont concernées.

franceinfo avec AFP
France Télévisions

Publié le 26/09/2022 16:36 Mis à jour le 26/09/2022 17:10 Temps de lecture : 5 min.



La façade du centre hospitalier sud-francilien de Corbeil-Essonnes (Essonne), le 23 septembre 2022. (EMMANUEL DUNAND / AFP)

Corbeil-Essonnes, sept. 2022

- Centre hospitalier
- Refus de payer la rançon
- 10% des données informatiques publiées sur le dark web

1. Cyber-risque : cas du rançongiciel

Neuchâtel Modifié le 31 mars 2022 à 20:43

Des milliers de données médicales neuchâteloises publiées sur le darkweb

Des hackeurs ont divulgué hier soir les données de milliers de patients neuchâtelois sur le darknet / 19h30 / 1 min. / le 30 mars 2022

Après un ultimatum, les pirates informatiques sont passés à l'acte mardi dans le canton de Neuchâtel: les données médicales de milliers de personnes se sont retrouvées en ligne sur le darkweb. Elles ont toutefois été retirées mercredi.

Neuchâtel, mars 2022

- 2 cabinets médicaux
- Refus de payer la rançon
- + de 43'000 de fichiers médicaux publiés sur le dark web

2. Enjeux: pour le médecin

- **Perte de productivité**
  - Ralentissement voire arrêt des consultations et traitements
  - Infrastructures potentiellement hors d'usage
- **Coûts liés directement à l'attaque informatique**
  - Négociations et rançon à payer
  - Audit informatique
  - Restauration des sauvegardes informatiques
  - Conseils juridiques

2. Enjeux: pour le médecin

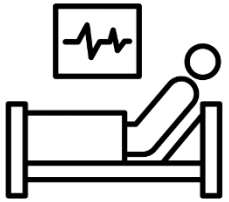
- Possible **perte de patientèle**
- **Sanctions** pénale, administrative voire associative
- **Responsabilité** civile et contractuelle du médecin

2. Enjeux: pour le patient

- **Atteinte à la vie privée**
  - Indisponibilité voire suppression définitive des données du patient
  - Divulgation à des tiers non autorisés
  - Usurpation d'identité

2. Enjeux: pour le patient

- **Atteinte à la santé voire la vie**



  - Risques d'erreur de diagnostic
  - Risques d'erreur de traitement
  - Risques accrus en cas d'intervention médicale en cours ou à venir
  - Possibles dysfonctionnements de dispositifs médicaux connectés (p.ex. pompe à insuline, défibrillateur)

2. Enjeux: pour le patient

- **Atteinte au patrimoine/liberté**
  - Réutilisation des données volées pour rançonner le patient

Octobre 2020

Cyber-attaques secondaires contre des milliers de patients en Finlande


Le Monde

Consulter le journal

Se connecter

ACTUALITÉS ÉCONOMIE VIDÉOS DÉBATS CULTURE LE GOÛT DU MONDE SERVICES

PIXELS • SÉCURITÉ INFORMATIQUE

La Finlande secouée par le piratage de milliers de dossiers de patients en psychothérapie

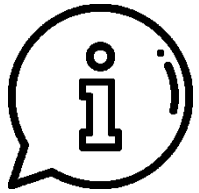
Des milliers de plaintes ont été déposées, les pirates ayant tenté de faire chanter des dizaines de patients. Le gouvernement a été réuni en urgence.

Le Monde avec AFP

Publié le 27 octobre 2020 à 18h35 • Mis à jour le 27 octobre 2020 à 18h49 • Lecture 3 min.

3. Obligation légale d'annoncer

- **Obligation légale** d'informer (art. 24 nLPD, dès sept. 2023)
  - Préposé fédéral à la protection des données et à la transparence (PFPDT)
  - le patient « *lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige* »
- **Contenu de l'annonce**: nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées
- **Délai** : « *dans les meilleurs délais* »



4. Risques juridiques

1. **Violation du secret médical (et secret de fonction?)**
2. **Violation des obligations découlant des lois sur la protection des données**
3. **Procès en responsabilité civile et contractuelle contre le médecin**

4. Risques juridiques

A. Violation du secret médical

- Révélation du secret à un tiers non-autorisé

→ Omission suffit (défaut de surveillance)

→ Acte intentionnel ou par négligence?

  - Droit pénal: seule l'intention est punissable
  - Droit disciplinaire/responsabilité civile: négligence suffit

4. Risques juridiques

- **Sanctions possibles et cumulables**

1. **Pénales** : peine privative de liberté de trois ans au plus ou peine pécuniaire (art. 321 CP)

2. **Disciplinaires** : avertissement, blâme, amende jusqu'à 20 000 francs, etc. (art. 43 LPMéd)

3. **Déontologique** : avertissement, blâme, amende jusqu'à 20 000 francs, etc. (art. 18 al. 14 Statuts AMGe, Code de déontologie de la FMH)

4. Risques juridiques

B. Violation d'obligations découlant des lois sur la protection des données

- **Art. 8 nLPD**: Obligation d'assurer une sécurité adéquate des données personnelles par rapport au risque encouru par des mesures organisationnelles et techniques appropriées

- **Violation intentionnelle** des exigences minimales de l'art. 8 nLPD (en vigueur dès sept. 2023)

  ➡ Amende jusqu'à CHF 250'000 (art. 61 let. c nLPD)

- Application possible du **RGPD**?

4. Risques juridiques

C. Procédure en responsabilité civile ou contractuelle du patient

- **Griefs**: violation du secret médical (y compris par négligence), atteinte à la santé ou à la personnalité, violation des règles de l'art médical

- Paiement de **dommages-intérêts?**

Conclusion

- La question n'est **pas** de savoir **si** l'on sera victime de cyber-risques, **mais quand**

- Le médecin doit démontrer **assurer une sécurité adéquate**

  - avoir réfléchi à la question, trouvé des solutions et pris les mesures préventives nécessaires

Merci pour votre attention