Guide:

Les Cabinets Médicaux Suisses :

Face à la Menace Cyber

Analyse de la situation et recommandations

Médilac
Consulting

Cyberattaques contre les Cabinets Médicaux en Suisse et Suisse Romande

1. Contexte suisse général

63K
Cyber incidents
enregistrés par l'OFCS en 2024

+13K
Augmentation
vs. 2023

8.5
Minutes
Un incident toutes les 8 min

12K
Cas de phishing
en 2024 (+2500 vs 2023)

Hôpitaux suisses dangereusement exposés (rapport NTC).

2. Cas majeur en Suisse romande : Cyberattaque Vidymed (décembre 2024)

Attaque Vidymed
Le 7 déc. 2024, le groupe Vidymed (Lausanne) est attaqué, impactant plus de 100 médecins indépendants.

Impact prolongé
Plus d'un mois sans accès (dossiers, agendas), entraînant des pertes financières (facturation).

Conséquences graves
Non-conformité légale et reconstruction manuelle des dossiers.

3. Incident historique 2022

Mars 2022 : Piratage de cabinets médicaux en Suisse romande.

Fuite de données : Dossiers patients sur le Darknet. Le PFPDT a constaté une sécurité insuffisante.

4. Menaces spécifiques

Ransomwares
Types : Akira, Black Basta.

Attaques sophistiquées
Plus ciblées et complexes (2025).

IA par les cybercriminels
Utilisation accrue de l'IA.

Phishing & fraudes
Téléphoniques (60%).

5. Vulnérabilités du secteur médical suisse

Failles informatiques
Systèmes hospitaliers avec failles majeures (rapport NTC).

Données non sécurisées
Données patients insuffisamment protégées.

Dépendance/Vulnérabilité
Dépendance aux systèmes centralisés et vulnérabilité des médecins indépendants.

Recommandations pour les Cabinets Médicaux Suisses

Cadre légal et organismes de référence

OFCS (Office fédéral de la cybersécurité)
Point de contact central pour la cybersécurité.

PFPDT (Préposé fédéral à la protection des données)
Garantit le respect des lois sur la protection des données et la confidentialité.

Obligation légale d'informer les patients
Communication transparente avec les patients en cas de violation.

Signalement obligatoire des incidents
Tous les incidents doivent être signalés aux autorités.

Mesures préventives prioritaires

Audits de sécurité réguliers
Évaluations fréquentes et approfondies des systèmes.

Sauvegardes externalisées et déconnectées
Copies de secours hors ligne et séparées.

Formation spécifique du personnel médical
Sensibilisation et formation continue aux menaces.

Éviter la dépendance à un seul système centralisé
Diversifier les solutions et les fournisseurs.

Mise en place de systèmes de détection précoce
Outils de surveillance et d'alerte en temps réel.

Spécificités pour médecins indépendants

Vérifier les garanties de sécurité des prestataires IT
S'assurer des normes de sécurité élevées des fournisseurs.

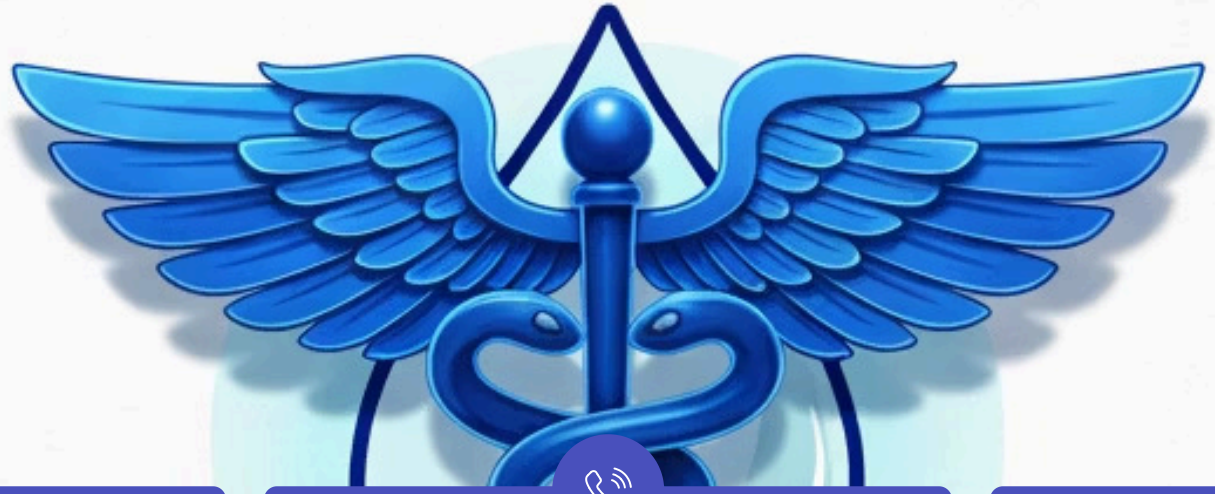
Maintenir des copies locales sécurisées des données critiques
Copies de sauvegarde indépendantes des systèmes cloud.

Prévoir un plan de continuité sans accès au système principal
Procédures manuelles ou alternatives pour les opérations essentielles.

Assurance cyber adaptée au secteur médical
Assurance spécifique couvrant les risques de cyberattaques.

Ressources et support

- **Portail OFCS : signalement et alertes**
  Plateforme pour signaler les incidents et recevoir des informations.
- **Veille active sur les menaces émergentes**
  S'informer des dernières vulnérabilités et techniques d'attaque.
- **Collaboration avec experts en sécurité IT santé**
  Faire appel à des spécialistes du domaine.



Email

vincent.limbach@medilac.ch

Téléphone

+41 79 393 80 13

LinkedIn

Profil LinkedIn

Médilac Consulting