Guide:

Cabinets Médicaux Suisses :

Face à la Menace Cyber

Analyse de la situation et recommandations 2024-2025

Médilac Consulting

Cyberattaques contre les Cabinets Médicaux en Suisse et Suisse Romande

1. Contexte suisse général

63K

Cyber incidents

enregistrés en 2024 par l'OFCS

+13K

Augmentation

par rapport à 2023

8.5

Minutes

Un incident signalé toutes les 8 minutes et demie

12K

Cas de phishing

en 2024 (+2'500 vs 2023)

Les hôpitaux suisses sont **dangereusement exposés** selon un rapport NTC.

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

Attaque Vidymed

Le 7 décembre 2024, le groupe Vidymed à Lausanne est attaqué.

Impact étendu

Plus de 100 médecins indépendants ont été impactés.

Perte d'accès

Plus d'un mois sans accès aux dossiers patients ni aux agendas.

Pertes financières

Impossibilité de facturer les services, entraînant des pertes salariales.

Non-conformité légale

Impossibilité d'informer les patients, non-respect des obligations légales.

Reconstruction manuelle

Reconstruction manuelle des dossiers devenue nécessaire.

3. Incident historique 2022

Mars 2022 : Piratage de cabinets médicaux en Suisse romande.

Fuite de données : Publication de nombreux dossiers patients sur le Darknet.

Constat : Intervention du PFPDT (Préposé fédéral à la protection des données) révélant des données médicales insuffisamment sécurisées en Suisse.

4. Menaces spécifiques

Ransomwares

(Akira, Black Basta)

Attaques sophistiquées

Plus ciblées et complexes en 2025.

IA par les cybercriminels

Utilisation accrue de l'intelligence artificielle.

Phishing & fraudes

Téléphoniques (60% des cas).

5. Vulnérabilités du secteur médical suisse

Systèmes informatiques hospitaliers avec failles majeures (rapport NTC).

Données patients non sécurisées de manière adéquate.

Dépendance aux systèmes informatiques centralisés.

Médecins indépendants particulièrement vulnérables.

Recommandations pour les Cabinets Médicaux Suisses

Cadre légal et organismes de référence

OFCS (Office fédéral de la cybersécurité)

Anciennement NCSC, il est le point de contact central pour la cybersécurité en Suisse.

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

En cas de violation, la communication transparente avec les patients est impérative.

Signalement obligatoire des incidents

Tous les incidents de cybersécurité doivent être signalés aux autorités compétentes.

Mesures préventives prioritaires

Audits de sécurité réguliers
Des évaluations fréquentes et approfondies des systèmes sont recommandées (rapport NTC).

Sauvegardes externalisées et déconnectées
Des copies de secours hors ligne et géographiquement séparées sont essentielles pour la reprise après incident.

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

Éviter la dépendance à un seul système centralisé
Diversifier les solutions et les fournisseurs pour réduire les risques de défaillance unique.

Mise en place de systèmes de détection précoce
Des outils de surveillance et d'alerte en temps réel pour identifier rapidement les tentatives d'attaque.

Spécificités pour médecins indépendants

Vérifier les garanties de sécurité des prestataires IT
S'assurer que les fournisseurs de services informatiques respectent les normes de sécurité élevées.

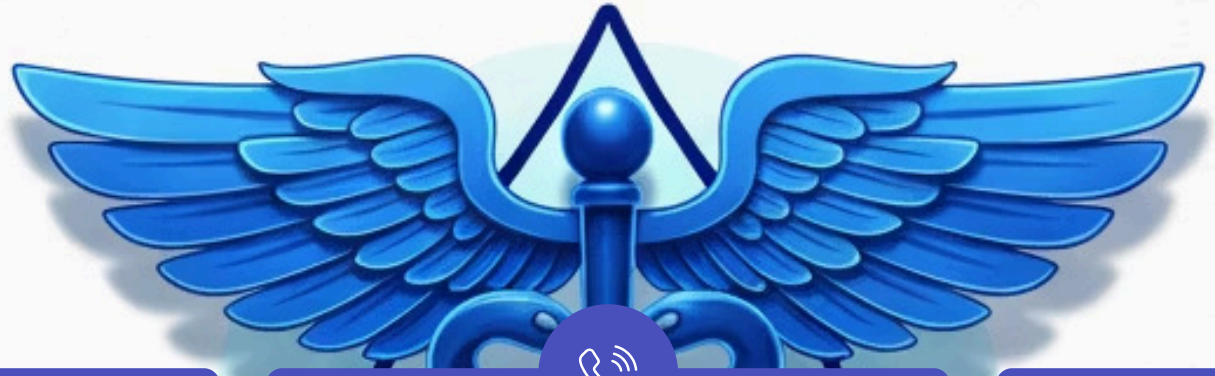
Maintenir des copies locales sécurisées des données critiques
Disposer de copies de sauvegarde indépendantes des systèmes cloud ou centralisés.

Prévoir un plan de continuité sans accès au système principal
Mettre en place des procédures manuelles ou alternatives pour les opérations essentielles.

Assurance cyber adaptée au secteur médical
Contracter une assurance spécifique couvrant les risques liés aux cyberattaques et aux fuites de données.

Ressources et support

- **Portail OFCS : signalement et alertes**
  Une plateforme pour signaler les incidents et recevoir des informations sur les menaces.
- **Collaboration avec experts en sécurité IT santé**
  Faire appel à des spécialistes du domaine pour des audits et des solutions personnalisées.
- **Veille active sur les menaces émergentes**
  Se tenir informé des dernières vulnérabilités et des techniques d'attaque utilisées par les cybercriminels.



Email

vli.partenaire@bs-associes.ch

Téléphone

+41 79 393 80 13

LinkedIn

Profil LinkedIn

Vincent

Limbach

Médilac Consulting