HORNETSECURITY BY proofpoint.

FACTSHEET

CYBERSÉCURITÉ DANS LE SECTEUR DE LA SANTÉ

La perturbation numérique dans la santé peut affecter la recherche, la prestation des soins, la confiance et la sécurité

Dans l'environnement de santé numérique actuel, du diagnostic et des traitements aux dossiers patients et à la facturation, tout repose sur des systèmes informatiques sécurisés et fiables. Une seule violation peut avoir des conséquences étendues : non seulement elle compromet des données sensibles de patients, mais elle perturbe aussi les opérations cliniques, retarde les traitements et, dans les cas graves, met des vies en danger. Contrairement à beaucoup d'autres secteurs, l'indisponibilité des systèmes dans la santé ne signifie pas seulement une perte de productivité et des coûts financiers, elle peut impacter directement la santé des patients, faisant de la cybersécurité un pilier de la qualité des soins.

Pourquoi la santé est-elle une cible majeure ?

» **Données à forte valeur :** les organisations de santé détiennent des informations personnelles riches, idéales pour l'usurpation d'identité, la fraude et l'extorsion

» **Urgence des soins :** la pression temporelle accroît la probabilité de payer une rançon pour rétablir rapidement les opérations

» **Facteur humain:** des équipes très sollicitées et une collaboration complexe augmentent l'exposition au phishing, à l'ingénierie sociale et aux fuites accidentelles

» **Infrastructures obsolètes :** les systèmes legacy et les environnements difficiles à corriger créent des failles exploitables

DONNÉES PATIENTS ET OPÉRATIONNELLES

- Dossiers patients et historiques médicaux
- Diagnostics, résultats de laboratoire, imagerie
- Détails d'assurance, de facturation et de paiement
- Identifiants du personnel, e-mails et documents internes

Confiance, crédibilité, réputation, confiance des parties prenantes

DONNÉES DE RECHERCHE

- Données et protocoles d'essais cliniques
- Jeux de données des participants à la recherche
- Données génomiques et biomarqueurs
- Résultats d'études et documents de collaboration

Intégrité de la recherche, marque employeur

03/26

HORNETSECURITY
BY proofpoint.

7,42 M$
coût moyen d'une violation de données dans la santé (secteur le plus coûteux pour la 14e année consécutive)

279 JOURS
durée moyenne pour identifier et contenir une violation dans la santé (la plus longue tous secteurs confondus, plus de 5 semaines au-dessus de la moyenne)

18 %
des attaques par ransomware dans la santé sont causées par des identifiants compromis

22 %
des attaques dans la santé sont causées par des e-mails malveillants

QUE SE PASSE-T-IL QUAND DES DONNÉES SONT VOLÉES ?

1. TROMPERIE
e-mail de phishing | faux identifiant | « demande urgente »

2. ACCÈS OBTENU
p. ex. via des identifiants volés

3. PROPAGATION
liens partagés
mouvement latéral

4. DONNÉES TROUVÉES
dossiers patients
fichiers de recherche

5. EXFILTRATION
copie discrète des données

6. PRESSION
fuites sur le dark web entraînant chantage | demandes de rançon | extorsion répétéev

RÉSERVEZ VOTRE DÉMO DÈS MAINTENANT

HORNETSECURITY
BY proofpoint.

10 BONNES PRATIQUES POUR PRÉVENIR LES VIOLATIONS DE DONNÉES

Évaluer et améliorer

1. Réalisez régulièrement des analyses de risques des systèmes, des appareils et des processus.
2. Testez les contrôles (simulez des attaques, validez la détection et les plans de réponse).

Réduire le risque humain

3. Formez le personnel en continu (p. ex., phishing, ingénierie sociale).
4. Faites vivre une culture « security-first » (canal de signalement clair).

Protéger l'accès et les systèmes

5. Mettez en œuvre des contrôles d'accès stricts fondés sur le principe du moindre privilège.
6. Utilisez l'authentification multifacteur (MFA) partout où c'est possible.
7. Corrigez et mettez à jour l'IT et les dispositifs médicaux.

Protéger et restaurer

8. Chiffrez les données sensibles.
9. Sauvegardez les systèmes et données critiques en appliquant une règle résiliente comme la 3-2-1-1.
10. Élaborez un plan de réponse aux incidents définissant clairement les rôles, les contacts et les priorités de reprise.

COMMENT HORNETSECURITY ACCOMPAGNE LE SECTEUR DE LA SANTÉ

Suite complète de sécurité cloud pour Microsoft 365 couvrant sécurité, conformité, sensibilisation et sauvegarde. Elle aide les organisations de santé à prévenir les incidents et à accélérer la reprise.

SECURITY AWARENESS	Renforcez votre « pare-feu humain » grâce à des formations ciblées et des simulations de phishing réalistes, pour réduire mesurablement la vulnérabilité aux attaques dans le temps.
ADVANCED THREAT PROTECTION	Protège contre les attaques sophistiquées (p. ex., spear-phishing, ransomware, exploits zero-day) au moyen de méthodes de détection avancées.
SPAM & MALWARE PROTECTION	Bloque les contenus e-mail malveillants avant qu'ils n'atteignent la boîte de réception du personnel, protégeant ainsi les communications cliniques et réduisant les risques liés à l'email.
365 TOTAL BACKUP	Permet une restauration rapide des données Microsoft 365 pour soutenir la continuité des soins et la conformité, tout en réduisant l'impact du ransomware et des suppressions accidentelles.
PERMISSION MANAGEMENT	Fait appliquer le moindre privilège dans Microsoft 365 et met en évidence les partages à risque et les erreurs de configuration.

hornetsecurity.com | info@hornetsecurity.com | +49 511 515 464-0