Les défis et les meilleures pratiques de la cybersécurité dans le secteur de la santé — 2e édition. Focus sur la gestion d'incidents

La montée en puissance des cyberattaques dans le secteur de la santé impose aux hôpitaux et établissements de soins une vigilance accrue et une préparation rigoureuse pour protéger les données critiques des patients tout en assurant la continuité des soins. Ce livre blanc, dans sa seconde édition, explore les défis et les meilleures pratiques de la cybersécurité à travers des témoignages d'établissements de santé wallons ayant été confrontés à des cyberattaques. Il met un accent particulier sur la gestion d'incidents et l'importance d'une réponse coordonnée.

1. **Un secteur de la santé vulnérable et exposé aux cybermenaces**

Les établissements de santé sont devenus des cibles de choix pour les cybercriminels en raison de la nature sensible des données qu'ils traitent et de l'importance des services qu'ils fournissent. La numérisation accrue des hôpitaux et des infrastructures de santé expose ces institutions à des attaques, dont les conséquences peuvent être catastrophiques, allant du vol de données sensibles à l'interruption des services critiques, avec des conséquences directes sur la sécurité des patients.

2. **Témoignages d'hôpitaux victimes de cyberattaques**

Des exemples comme ceux du **CHRSM** et de la **Clinique Saint-Luc Bouge** illustrent comment des hôpitaux ont été paralysés par des attaques de type ransomware. En dépit de l'ampleur de ces crises, ces établissements ont pu compter sur des communications proactives, une gestion de crise efficace et une mobilisation rapide des ressources internes et externes pour limiter les impacts sur les patients et les services essentiels.

3. **L'importance du facteur humain dans la gestion des incidents**

Les témoignages montrent que l'engagement des équipes, couplé à une gestion humaine de la crise, a été un facteur clé pour restaurer la normalité en seulement quelques jours. L'adoption de méthodes manuelles et la capacité à réagir rapidement ont permis aux équipes soignantes de poursuivre les soins, même en l'absence de systèmes informatiques opérationnels. **La préparation et la formation** jouent un rôle central dans la résilience des hôpitaux face à ces menaces.

4. **Un accompagnement essentiel pour une gestion efficace des incidents**

Le **Centre pour la Cybersécurité Belgique (CCB)**, via le **CERT**, est un partenaire stratégique dans la gestion des cyberattaques. Leur rôle, dès les premières heures d'une attaque, consiste à contenir la menace et à fournir des recommandations techniques pour la restauration des systèmes. L'usage d'outils **Cyberwal** tels que le **simulateur numérique** et la **Cyber Response Team (CRT)** permet aux hôpitaux dans le premier cas, de se préparer et de mieux gérer les crises lorsqu'elles surviennent et dans le cas du deuxième outil, d'apporter un soutien direct au CERT national en cas d'incident.

5. **Recommandations et stratégies pour renforcer la cybersécurité**

Ce livre blanc met en avant l'importance de **stratégies de cybersécurité robustes**, telles que l'authentification multifactorielle, la segmentation des réseaux et des plans de sauvegarde adaptés pour assurer une reprise rapide après un incident. La gestion des incidents doit s'appuyer sur des plans de continuité des opérations bien définis, adaptés à la taille et aux ressources des établissements. Les **leçons tirées** des incidents précédents soulignent la nécessité d'une **analyse post-incident** approfondie pour renforcer les défenses et améliorer les pratiques de cybersécurité à long terme.

6. **Une feuille de route claire et pratique**

Enfin, ce livre blanc propose une **feuille de route claire et pratique** pour les hôpitaux et établissements de santé afin de se préparer efficacement aux cyberattaques et réagir de manière appropriée en cas de crise. Grâce à des recommandations concrètes, il offre des outils et stratégies pour anticiper les menaces, protéger les infrastructures critiques et assurer la continuité des soins dans un environnement de plus en plus menacé par les cyberattaques.