Institut national de test pour la cybersécurité

COMMUNIQUÉ DE PRESSE

Le NTC identifie de importantes vulnérabilités dans les systèmes d'information hospitaliers (SIH) et publie des recommandations

Zoug, le 23 janvier 2025 – L'Institut national de test pour la cybersécurité NTC a procédé à une analyse technique de sécurité approfondie de trois systèmes d'information hospitaliers (SIH) couramment utilisés dans plusieurs hôpitaux suisses. Les fabricants ont été informés et des mesures ont été prises en vue de minimiser les risques. Le rapport publié met en évidence des vulnérabilités importantes et contient des recommandations concrètes sur les mesures à prendre afin d'améliorer la cybersécurité dans le secteur de la santé.

Les systèmes d'information hospitaliers sont au cœur des hôpitaux modernes. Ils gèrent le flux d'informations, traitent les données sensibles des patients et assurent le bon déroulement des opérations dans l'environnement hospitalier. L'examen du NTC a révélé que la cybersécurité de ces systèmes essentiels est insuffisante dans bon nombre de cas.

Résultats de l'analyse
D'importantes failles ont été constatées dans tous les systèmes examinés. Au total, plus de 40 vulnérabilités avec des niveaux de gravité moyens à élevés ont été identifiées, dont trois présentant la criticité la plus importante. Les solutions qui reposent sur des architectures obsolètes sont particulièrement vulnérables. Des problèmes fondamentaux liés à l'architecture, l'absence d'un cryptage ou sa mise en œuvre incorrecte, des systèmes connexes vulnérables et une séparation insuffisante entre les environnements de test et de production sont les principaux obstacles.

Certaines des failles identifiées permettaient d'accéder à l'ensemble des systèmes et des données des patients en l'espace de quelques heures. Si la plupart des failles constatées ont été corrigées entre-temps ou comblées par des mesures d'atténuation, certains problèmes fondamentaux nécessitent une refonte complète de l'architecture logicielle, ce qui, d'après les fabricants, prendra plusieurs années. En outre, l'analyse a permis de détecter plusieurs failles importantes dans des systèmes connexes qui n'entraient pas dans l'étendue définie du contrôle, mais qui ont été découvertes fortuitement en raison de leur caractère flagrant.

Le rapport renonce délibérément à fournir des détails sur les failles. En revanche, une information générale a été diffusée via le NTC Vulnerability Hub et une notification ciblée des hôpitaux concernés a été envoyée via le Cyber Security Hub (CSH) de l'Office fédéral de la cybersécurité (OFCS).

Recommandations pour les hôpitaux
Le rapport contient huit recommandations principales visant à améliorer durablement la cybersécurité dans les hôpitaux suisses. Il s'agit notamment de prendre en compte les exigences en matière de cybersécurité dès l'étape de l'acquisition de l'informatique et de réaliser des analyses de vulnérabilité régulières en vue d'un contrôle continu. En particulier dans les petits hôpitaux, les responsabilités en matière de cybersécurité doivent être clairement définies et les ressources nécessaires doivent être mises à disposition. Il est également recommandé de renforcer la mise en réseau entre les hôpitaux et d'accéder au Cyber Security Hub (CSH) de l'Office fédéral de la cybersécurité (OFCS).

Les résultats mettent en évidence la nécessité de procéder à des contrôles de sécurité réguliers et de définir clairement les responsabilités. Nous tenons à remercier tout particulièrement les hôpitaux et les organisations dont l'engagement dans le domaine de la cybersécurité a largement contribué à la réussite de cette analyse de sécurité.

Vers le rapport

Contact presse:
Andreas W. Kaelin, Directeur général
+41 41 317 00 11, andreas.kaelin@ntc.swiss

À propos de l'Institut national de test pour la cybersécurité NTC
L'Institut national de test pour la cybersécurité NTC contribue à la sécurité et à la souveraineté numérique de la Suisse en identifiant de manière anticipée les points faibles critiques et en encourageant leur correction. En tant qu'association à but non lucratif dont le siège est à Zoug, le NTC repose sur des principes d'indépendance et d'objectivité. Il effectue des tests de cybersécurité sur les infrastructures, les appareils et les applications en réseau qui revêtent une grande importance pour la société et l'économie.
https://fr.ntc.swiss/