DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Secteur médical et cybercriminalité

Prendre soin de la cybersécurité est bon pour la santé

Du fait de la numérisation de toutes les activités de la santé, les actrices et acteurs de la chaîne de soin sont désormais exposé-es à la cybercriminalité. Les données stockées, transmises, traitées par les systèmes d'information sont des valeurs convoitées.

Sans une informatique et des télécommunications opérationnelles, les activités médicales ne peuvent se réaliser. Dans le domaine de la santé, cela concerne tout aussi bien la partie administrative que celle directement ou non liée au soin. C'est la dépendance à l'informatique qui fragilise le secteur médical.

Un milieu attractif pour les cybercriminel-les

Tout ce qui est connectable à Internet est piratable. Les cyberattaques visent à faire dysfonctionner, modifier, voler, détruire des ressources informatiques.

Dans le monde médical, dans la mesure où l'informatique y est omniprésente, tous les systèmes connectés sont devenus des cibles privilégiées de cyberattaques consistant à les rendre inopérants. Sans compter le vol de données afin d'exercer un chantage portant sur la disponibilité des infrastructures numériques et sur la confidentialité des données.

Internet est un catalyseur d'actions abusives ou illicites et un vecteur de propagation de virus informatiques et d'actions relevant de l'escroquerie, de la fraude, du chantage, de la désinformation, ou encore de la surveillance et de l'espionnage.

Du vol de données jusqu'à la mort

Données de santé et systèmes médicaux sont des sources d'enrichissement. Les cybercriminel-les sont rationnel-les et s'attaquent préférentiellement aux cibles les plus vulnérables, aux structures les moins bien protégées quelle que soit leur taille. Ils et elles s'adaptent aux possibilités de leurs victimes en personnalisant schémas d'extorsion et demandes de rançons. Les préjudices sont variables en fonction de la nature, de l'intensité et de l'ampleur des cyberattaques. Du vol de données personnelles à des attaques majeures sur des infrastructures critiques, toute une gamme de nuisances existe pouvant conduire à l'impossibilité des soignant-es à réaliser leurs tâches, à la dégradation de la qualité des soins et à des pertes de vie humaine.

La sécurité des patient-es, le secret médical et le bien-être dépendent aussi de la disponibilité des systèmes informatiques, de l'intégrité et de la confidentialité des données. La cybersécurité contribue à protéger la vie humaine et la réputation des actrices et acteurs, ainsi qu'à offir un environnement de travail et de soin adapté. Il convient de doter les institutions d'une cybersécurité qui permette de réaliser ses missions en se protégeant des erreurs, des pannes et des malveillances liées aux technologies du numérique.

A lire

La Prof. Ghernaouti est l'auteure de « La Cybersécurité pour tous », Editions Slatkine, 2022

Ce contenu peut être utilisé dans un cadre privé ou pour la formation postgraduée et continue. Toute autre utilisation est subordonnée à l'autorisation écrite préalable de la Société Vaudoise de Médecine (SVM), éditrice et détentrice exclusive des droits.

DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Prof. Solange Ghernaouti
Directrice Swiss Cybersecurity Advisory & Research Group, UNIL

Ce contenu peut être utilisé dans un cadre privé ou pour la formation postgraduée et continue. Toute autre utilisation est subordonnée à l'autorisation écrite préalable de la Société Vaudoise de Médecine (SVM), éditrice et détentrice exclusive des droits.