e·sculape
informatique médicale

A nos client-e-s Mediway et infrastructure

Givisiez, le 1er avril 2022

Sécurité informatique

Madame, Monsieur,
Chère cliente, cher client,

En date du 22 mars dernier, nous vous écrivions pour vous informer de la situation concernant les attaques informatiques par rançongiciels, les améliorations de sécurité informatique mises en place et la vigilance nécessaire au sein de votre cabinet.

Suite aux articles de presse et reportages RTS mentionnant la publication de données médicales de patient-e-s sur le darknet, nous jugeons utile de vous revenir.

Par ce courrier, nous tenons à vous faire parvenir la déclaration complète qui a été transmise hier aux journalistes qui nous ont contactés, le message ayant été repris que très partiellement dans le TJ du soir de la RTS :

> A notre connaissance à ce jour, trois cabinets médicaux sis sur le canton de Neuchâtel ont été attaqués par un même rançongiciel.
>
> Les données médicales publiées le 31 mars sur le darknet dont nous avons pu avoir connaissance sont issues d'un seul des cabinets visés. Aucun document n'est issu du logiciel médical Mediway utilisé actuellement par le cabinet. Les données sont issues d'une autre source, utilisée antérieurement.
>
> Dès la connaissance des attaques, nous avons opéré avec effet immédiat un renforcement de la sécurité chez nos clients. Un courrier d'information leur a été adressé le 22 mars pour les informer de ces efforts et leur rappeler la nécessité de participer activement à la sécurité informatique à nos côtés.
>
> Mediway est un logiciel utilisé dans de nombreux cabinets en Suisse romande. Les standards de sécurité sont très élevés, avec une base de données cryptée à différents niveaux et un chiffrement fort. En tant que distributeur de ce produit, nous n'avons à ce jour pas eu d'écho de fuite de données en lien avec ce logiciel. Nous travaillons en collaboration très étroite, aussi bien avec le développeur du logiciel et les différents partenaires, ainsi qu'avec une société spécialisée dans la cybersécurité sise à Genève, afin que cela reste le cas.

T +41 26 550 05 80
F +41 26 550 05 81
info@e-sculape.ch
Rte André Piller 21
1762 Givisiez
www.e-sculape.ch

e·sculape
informatique médicale

Nous pouvons vous assurer de la transparence de cette information et de la vigilance constante de l'équipe de développement du logiciel Mediway, en tout temps et particulièrement depuis ces dernières actualités.

Concernant la sécurité globale de votre réseau informatique :
La faille de sécurité qui a été utilisée par les hackers a été identifiée. Il s'agit chaque fois de la même faille. Nous avons une liste des cabinets concernés par le matériel incriminé. Ces cabinets ont, avec ce présent courrier, une lettre complémentaire.
Dans la mesure où vous n'avez pas de second courrier lié à celui-ci, vous avez l'assurance que votre cabinet n'a pas le matériel informatique contenant la faille utilisée pour les attaques de février et mars.

En complément des mesures de sécurité que nous mettons en place pour éviter toute nouvelle intrusion dans les réseaux informatiques de nos client-e-s, à la lumière des dernières informations que nous avons pu obtenir, soit que les données publiées sur le darknet sont des données médicales antérieures à l'utilisation du logiciel Mediway, nous vous invitons à contrôler si vous avez des données médicales stockées en-dehors de Mediway. Il peut s'agir de données antérieures à l'utilisation de Mediway, de logiciels précédemment utilisés auxquels vous avez encore accès, ou de fichiers contenant des informations de vos patient-e-s qui sont enregistrés dans des dossiers, sur votre serveur.
Concernant les logiciels médicaux autres que Mediway, nous vous invitons à vous renseigner sur leur sécurité et, au besoin, envisager une reprise des données dans Mediway et une suppression de tout ancien fichier.
Concernant les documents médicaux qui ne seraient pas intégrés dans Mediway, il serait utile de préciser l'utilisation et le temps durant lesquels ces documents restent sur votre réseau de manière non cryptée. Dans les processus de travail au sein du cabinet, il est nécessaire de tenir compte que seuls les documents insérés dans Mediway et supprimés de leur emplacement d'origine sont protégés par le cryptage de Mediway.

Nous vous invitons également encore une fois à faire usage de mots de passe complexes et à les changer régulièrement.
Un mot de passe complexe contient au minimum 8 caractères, composé d'au moins une majuscule, une minuscule, un chiffre et un caractère spécial (par ex : @, $, £, #).
La marche à suivre pour changer son mot de passe Windows est : Appuyer sur CTRL+ALT+Suppr (ou delete) / modifier un mot de passe.
La marche à suivre pour changer son mot de passe Mediway est : Clic sur l'onglet « ? » / Réinitialiser / Mot de passe.

Afin de maintenir la confiance qui nous lie, nous nous engageons à vous informer dans les meilleurs délais si de nouvelles informations devaient contredire les affirmations en lien avec la sécurité de Mediway que nous avançons dans ce courrier ou s'il devait y avoir découverte d'une autre faille de sécurité.

Avec nos cordiales salutations,

e-sculape informatique médicale s.a.

Jérôme Clément	Sophie Truffer	Mathias Maldonado
Directeur	Team Mediway	Team IT

T +41 26 550 05 80
F +41 26 550 05 81
info@e-sculape.ch
Rte André Piller 21
1762 Givisiez
www.e-sculape.ch