

# Cybercriminalité – le danger sous-estimé

Les risques et les menaces liés aux attaques de pirates informatiques augmentent, en particulier dans le secteur de la santé. La sensibilisation et la responsabilisation des professionnels de la santé, ladite «Awareness», joue un rôle de plus en plus important.

Un membre du personnel soignant d'une maison de retraite et de soins essaie de démarrer l'ordinateur le matin. Mais plus rien ne marche. Les fichiers ont été cryptés à l'aide d'un cheval de Troie dit crypto – aussi bien les données administratives que la documentation électronique des soins sont affectées. La maison de retraite a rapidement besoin de l'aide professionnelle de spécialistes en informatique. Difficile de ne pas penser aux coûts et à l'agacement des personnes touchées...

Avec ses données sensibles, le monde de la santé, en particulier, est de plus en plus la cible d'attaques de pirates informatiques. La formation des employés et la protection des équipements sont des priorités absolues pour éviter de telles cyberattaques. En tant que partenaire pour la sécurité intégrale, Health Info Net AG (HIN) offre des solutions adaptées à chaque institution pour augmenter considérablement la protection contre le vol et la manipulation de données, contre les escroqueries financières ou même le chantage.

## Services HIN pour la sécurité informatique et la sensibilisation



### Formation HIN Awareness

La formation de sensibilisation Awareness personnalisable par un expert en sécurité informatique HIN sur place renforce la prise de conscience des risques de vos collaborateurs, souligne les mesures de protection et augmente ainsi la sécurité de l'information de votre institution.

Pour plus d'informations: [www.hin.ch/awareness-schulung](http://www.hin.ch/awareness-schulung)



### HIN Awareness Portal

HIN offre un outil d'e-learning pour les formations régulières. Grâce au HIN Awareness Portal, vous pouvez vous sensibiliser de manière ciblée, ainsi que vos collaborateurs, au moyen de différents modules, et ce indépendamment du lieu et de l'heure.

Informations supplémentaires: [www.hin.ch/awareness-portal](http://www.hin.ch/awareness-portal)

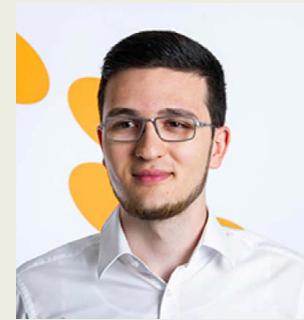


### HIN Endpoint Security Service (EPS)

Protégez vos appareils de manière globale contre les menaces provenant d'Internet. L'EPS fournit un logiciel de protection de pointe pour vos outils de travail, complété par le HIN Security Operation Center. En cas d'urgence, vous serez pris en charge de manière proactive par des experts en sécurité expérimentés.

Informations supplémentaires: [www.hin.ch/endpoint](http://www.hin.ch/endpoint)

## Entretien avec Oussama Zgheb



«Le meilleur détecteur de virus est inutile si les collaborateurs ne sont pas sensibilisés.»

### Monsieur Zgheb, que peuvent faire les institutions pour se protéger contre la cybercriminalité?

Je recommande une combinaison de mesures éprouvées afin de maintenir un niveau de protection si élevé qu'une attaque n'en vaudrait pas la peine pour un pirate informatique.

### A quoi devrait ressembler une telle combinaison?

Des mesures techniques telles qu'un pare-feu sont indispensables. Au niveau organisationnel, les processus devraient être établis et contrôlés de manière centralisée. Le troisième élément concerne les mesures comportementales telles que la gestion sécurisée des mots de passe. Le plus important reste la formation: le meilleur détecteur de virus est inutile si les collaborateurs ne sont pas sensibilisés.

### Comment sensibiliser les collaborateurs au quotidien?

La formation par un expert est un bon moyen de sensibiliser les collaborateurs. Afin d'ancrer durablement les connaissances, il est important de veiller à ce que les collaborateurs reçoivent une formation continue régulière, par exemple à l'aide d'un outil d'e-learning.

*Oussama Zgheb est expert en sécurité informatique chez Health Info Net AG (HIN)*