relyens
GROUPE MUTUALISTE EUROPÉEN
ASSURANCE ET MANAGEMENT DES RISQUES
sham | sofaxis | neeria

sham
PARTAGEONS PLUS QUE L'ASSURANCE
une société du groupe relyens

Communiqué de presse

Lyon, le 8 février 2021

Face à la menace croissante, Sham (groupe Relyens) décrypte dans un Livre Blanc les enjeux techniques et financiers de la cybersécurité dans les établissements de santé et médico-sociaux

Sham, Manager des risques partenaire des acteurs de la santé et du médico-social à l'échelle européenne, publie un Livre Blanc consacré à leur cybersécurité. Dysfonctionnements, attaques, impact de la crise sanitaire, gouvernance, obligations et bonnes pratiques… Sham décrypte le risque cyber à travers les témoignages d'experts en cybersécurité et chiffres clés, et appelle à mieux préparer la cyber résilience des établissements.

La cybersécurité : un enjeu majeur pour les établissements de santé et médico-sociaux

Dans les établissements de santé, les dysfonctionnements ou la moindre cyberattaque peuvent avoir des conséquences tragiques comme des perturbations d'activité, un non accès aux données des patients pouvant mener à des pertes de chance ou des erreurs médicales. L'augmentation de la digitalisation des outils et activités stratégiques des établissements, la réorganisation en urgence des établissements de santé pendant la crise Covid-19, entraînant une multiplication de « bris de glace », jouent un rôle déterminant dans la multiplication des risques cyber en santé.

Selon le Rapport d'activité 2019 de l'Agence du Numérique en Santé, 300 établissements ont déclaré 392 incidents en 2019, soit une augmentation de 20 % par rapport à 2018. **43 % des incidents signalés en 2019 ont une origine malveillante**, avec comme vecteurs d'attaques principaux le courrier électronique et le logiciel malveillant, avec notamment une croissance significative des attaques par rançongiciels (+ 40 % par rapport à 2018)[1].

Le secteur médico-social, moins mature sur le volet numérique, est aussi moins protégé face aux cyberattaques ou aux dysfonctionnements informatiques internes.

Dans ce contexte, la cybersécurité devient alors une condition nécessaire et permanente de la confiance dans le système de santé.

[1] *Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (Rapport public 2019)*

Les établissements doivent devenir cyber résilients

Une structure cyber résiliente est capable de mieux réagir et d'être mieux protégée, de façon à ce que son activité ne se retrouve pas sévèrement et durablement impactée.

Cela passe par davantage d'investissements et une gouvernance renforcée. Les structures de santé n'ont pas encore toutes investi dans cette résilience, même si elle est nécessaire et obligatoire. Elles y sont néanmoins contraintes car outre le coût financier, induit par un incident numérique, les conséquences en termes de réputation peuvent être désastreuses.

L'enjeu de gouvernance exige des décideurs, considérant souvent la cybersécurité comme une fonction support, d'intégrer désormais la protection des données au cœur de leur stratégie opérationnelle. Le RSSI et le DSI doivent donc se concerter pour démontrer l'impact des problèmes technologiques sur les activités métiers. Les cyber menaces ne sont pas uniquement des défis techniques à relever, elles représentent des enjeux critiques à communiquer au conseil d'administration dans un langage compréhensible : risques, opportunités et avantages financiers.

« Le risque cyber s'aggrave dans les établissements de santé et du médico-social, en France comme à l'étranger. Face à cette situation, le métier de Sham s'adapte et évolue vers une approche plus holistique de la gestion du risque cyber : de l'évaluation et du conseil préventif en amont, à la proposition de solutions et jusqu'à l'accompagnement, dès les premiers instants en cas de crise, pour atténuer ses impacts. Face à la menace numérique croissante, il est temps de se mettre ensemble en ordre de bataille sur le plan technique et organisationnel dans l'intérêt de tous. »
Lionel Prades, Responsable Risques Technologiques du groupe Relyens

Anticipation et prévention : le Management des risques cyber selon Sham

Manager des risques partenaire des acteurs de la santé et du médico-social en Europe, Sham accompagne les dirigeants et les RSSI sur la gestion globale des risques cyber en associant une offre de prévention unique s'appuyant sur des partenaires technologiques de premier plan, CyberMDX et Advens (en France), à une offre assurantielle enrichie pour faire face aux sinistres.

Pour en savoir plus :

- Télécharger le Livre Blanc « *Cybersécurité, le nouveau défi des établissements de la santé et du médico-social - Edition 2021* » ici.

LES CHIFFRES DU RISQUE CYBER DANS LA SANTÉ EN FRANCE

DES INCIDENTS AVAIENT POUR ORIGINE DES INTERRUPTIONS DE SERVICES OU DES DYSFONCTIONNEMENTS

(bugs d'applications métier, défaillances de services opérateur ou de réseaux internes ou même de plateformes d'hébergeurs)

Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (Rapport public 2019)

DES INCIDENTS SONT D'ORIGINE NON MALVEILLANTE

conséquence de pannes d'opérateurs télécom, d'interruptions de service non programmées, de dégradations physiques de l'infrastructure...

Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (Rapport public 2019)

DES INCIDENTS ONT UNE ORIGINE MALVEILLANTE

avec comme vecteurs d'attaques principaux le courrier électronique et le logiciel malveillant, notamment une croissance significative des attaques par rançongiciels **(+ 40 % PAR RAPPORT À 2018)**

Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (Rapport public 2019)

43 %

DES INCIDENTS ONT UN IMPACT SUR DES INFORMATIONS PATIENT À CARACTÈRE PERSONNEL

et 11 % d'entre eux ont ou auraient pu entraîner une mise en danger de la vie des patients.

Source : cyberveille-sante.gouv.fr

55

STRUCTURES DE SANTÉ

ont déclaré plus de 2 incidents en 2019, 7 d'entre elles ayant signalé plus de 4 incidents.

Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (Rapport public 2019)

120

ÉTABLISSEMENTS DE SANTÉ

soit tout le réseau d'un grand groupe privé français, ont été atteint par une cyberattaque à l'été 2019. Les dysfonctionnements ont duré une semaine.

Source : Anssis

A propos de Sham

Créée en France en 1927 par des directeurs d'hôpitaux, Sham, société mutuelle spécialisée dans l'assurance et le management des risques, est depuis plus de 90 ans le partenaire solide et durable des acteurs de la santé et du médico-social. Opérateur de référence européen en matière de responsabilité civile, Sham compte près de 11 000 sociétaires – établissements et professionnels. Basée en France (siège social à Lyon), en Espagne, en Italie et en Allemagne, Sham emploie près de 550 personnes et a réalisé 422 M€ de chiffre d'affaires en 2019.
www.sham.fr
Twitter : @Sham_France
LinkedIn : SHAM

Sham est la société de tête de Relyens, groupe mutualiste européen de référence en assurance et management des risques auprès des acteurs de la santé et des territoires exerçant une mission d'intérêt général. Avec plus de 1 000 collaborateurs, plus de 30 000 clients et sociétaires, et près de 900 000 personnes couvertes dans 4 pays (France, Espagne, Italie et Allemagne), Relyens a collecté 891 M€ de primes, pour un chiffre d'affaires de 484 M€ en 2019. Le Groupe, fortement ancré dans ses environnements clients à travers ses marques Sham, Sofaxis et Neeria, développe des solutions globales sur mesure combinant solutions d'assurances (assurances de personnes et de biens) et services en management des risques.
www.relyens.eu
Twitter : @Relyens
LinkedIn : Relyens
Youtube : RELYENS

Contact presse : Agence Ekno : Xavier Cayon – 06 23 12 63 46 – xavier.cayon@ekno.fr