HORNETSECURITY

INFOSHEET
AI POWERED

SECURITY AWARENESS SERVICE

SERVICE DE SENSIBILISATION À LA SÉCURITÉ POUR LES ORGANISMES DE SANTÉ

Les cybermenaces dans le secteur de la santé ne cessent de s'intensifier à mesure que l'erreur humaine, les vulnérabilités numériques et les chaînes d'approvisionnement complexes mettent en péril les données essentielles. Des initiatives intégrées en matière de cybersécurité combinées à une formation de sensibilisation à la sécurité sur mesure permettent à votre équipe de renforcer les défenses et de protéger les services essentiels.

LES MENACES CROISSANTES POUR LE SECTEUR DE LA SANTÉ

Les organismes de santé sont de plus en plus souvent la cible de cyberattaques, avec plusieurs attaques majeures et des tendances récentes telles que :

- L'augmentation des cyberincidents : en 2023, les cyberincidents dans le secteur de la santé ont presque quadruplé, exposant plus de 133 millions de dossiers dans 725 violations.
- Les perturbations dues aux rançongiciels : des attaques telles que l'incident Change Healthcare et d'autres ont montré comment les rançongiciels peuvent retarder des procédures médicales critiques, créer un engorgement des salles d'urgence et compromettre la sécurité des patients.
- Les vulnérabilités liées à l'expansion numérique : à mesure que les hôpitaux adoptent davantage d'outils numériques - dossiers médicaux électroniques, télémédecine, diagnostics IA, etc. - le nombre de points d'entrée potentiels pour les cybercriminels augmente.
- Les risques liés à la chaîne d'approvisionnement et à la conformité : L'interdépendance des systèmes numériques et la pression exercée pour satisfaire à des réglementations strictes en matière de cybersécurité ont rendu la cybersécurité des soins de santé encore plus complexe.

Ces défis compromettent non seulement les soins aux patients, mais exposent également les organisations à des risques financiers et de réputation importants.

PASSEZ À L'ACTION DÈS AUJOURD'HUI

Ne laissez pas les cybermenaces compromettre vos services de santé. Donnez à votre équipe la défense proactive dont elle a besoin.

PROGRAMMEZ UNE DÉMO !

SECURITY
AWARENESS SERVICE

ACTION DE L'UE : UNE DIRECTIVE POUR DES MESURES PROACTIVES DE CYBERSÉCURITÉ

En réponse à ces menaces croissantes, la Commission européenne a dévoilé un plan d'action exhaustif visant à renforcer la cybersécurité dans les services de santé. Les principaux aspects de ce plan sont les suivants :

- Conseils de prévention et aide financière : offrir des crédits de cybersécurité et des conseils personnalisés pour aider les hôpitaux à établir des défenses plus solides.
- Détection des menaces et réaction rapide : proposition d'un système d'alerte rapide à l'échelle de l'UE et d'un centre de soutien à la cybersécurité dédié aux services de santé.
- Coopération internationale : utiliser des outils tels que la boîte à outils de la cyberdiplomatie pour décourager les cyberactivités malveillantes.

L'IMPORTANCE DE LA SENSIBILISATION À LA SÉCURITÉ

95 % des incidents de cybersécurité sont dus à une erreur humaine. Les employés sont la première ligne de défense contre les cybermenaces. Une formation complète de sensibilisation à la sécurité peut :

- Responsabiliser le personnel : donnez à chaque membre de l'équipe les connaissances nécessaires pour identifier et atténuer les menaces telles que le phishing et les rançongiciels.
- ictes en matière de cybersécurité.
- Réduire les perturbations : empêchez les retards dans les services de santé critiques en minimisant le risque de cyberattaques réussies.
- Protéger les données des patients : protégez les informations sensibles qui constituent l'élément vital des soins et de la confiance des patients.

SECURITY AWARENESS SERVICE: LE PARTENAIRE DE CYBERDÉFENSE DU SECTEUR DE LA SANTÉ

Hornetsecurity propose un service de sensibilisation à la sécurité de pointe conçu pour protéger les organisations dans un large éventail de secteurs, y compris les services de santé. Voici comment notre solution fait la différence :

- Des programmes de formation sur mesure : des modules personnalisés abordent les défis uniques de la cybersécurité dans le secteur de la santé, garantissant que votre personnel est prêt à faire face aux menaces du monde réel.
- Un contenu exhaustif : de la navigation sécurisée sur Internet au traitement sécurisé des informations de santé personnelles, notre formation couvre tous les sujets essentiels.
- Une facilité de mise en œuvre : notre service est conçu pour s'intégrer de manière transparente dans vos systèmes existants, réduisant ainsi les temps d'arrêt et augmentant la résilience globale.
- Un soutien continu : des mises à jour et des suivis continus permettent à votre organisation de garder une longueur d'avance sur l'évolution des cybermenaces.