#DemainDigital

VERS LA TRANSFORMATION NUMÉRIQUE

en collaboration avec digital wallonia .be

CYBERWEEK EN WALLONIE

CYBERSÉCURITÉ : LE SECTEUR DE LA SANTÉ AU CŒUR DE LA SENSIBILISATION

Du 14 au 18 octobre, l'Agence du Numérique, à travers son programme Cyberwal by Digital Wallonia, organise la Cyberweek, une semaine chargée de sensibiliser divers secteurs, dont celui de la santé, aux enjeux de la cybersécurité.

Sensibiliser le secteur de la santé aux enjeux de la cybersécurité est devenu d'autant plus nécessaire que les chiffres de la cybercriminalité le concernant directement sont inquiétants.

La cybersécurité est devenue un challenge pour toutes les entreprises, quelle que soit leur taille et c'est d'autant plus vrai pour le secteur de la santé, que l'on parle de petites structures ou de grands établissements hospitaliers, avec notamment en ligne de mire les dossiers médicaux des patients et toutes sortes de données dites sensibles qui pourraient se monnayer sur le darknet.

« En Belgique, le secteur de la santé est passé de 1.607 attaques par semaine à 1.795 pour 2023. 65 % des tentatives d'attaques sont parvenues par courrier électronique et 35 % via le web », explique Nina Hasratyan, experte en cybersécurité auprès de l'Agence du Numérique (AdN).

NIVEAUX DE MATURITÉ DIFFÉRENTS

Cyberwal by Digital Wallonia, qui incarne l'ambition de la Wallonie en matière de cybersécurité, a d'ailleurs placé la santé parmi ses secteurs prioritaires, au même titre que l'industrie, le secteur public ou les PME. « Dans le secteur de la santé, des efforts considérables ont été consentis, avec les acteurs-clés du système pour cibler les grandes structures comme les hôpitaux mais aussi les plus petites comme les maisons de repos. L'approche est différente tout comme les niveaux maturité », ajoute-t-elle.

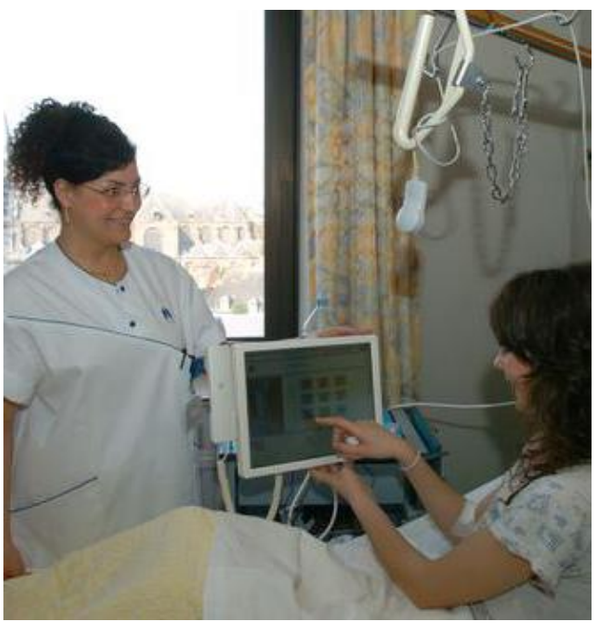
> La cybersécurité est devenue un challenge pour toutes les entreprises, quelle que soit leur taille et c'est d'autant plus vrai pour le secteur de la santé

Le programme organise donc, du 14 au 18 octobre 2024, la Cyberweek, dans plusieurs villes wallonnes. Cette semaine sera ponctuée par divers événements (ateliers, conférences...) avec l'objectif de mettre en mouvement les différents secteurs face aux défis posés par la cybersécurité.

« La situation évolue, les entreprises commencent à se protéger mais cela ne progresse pas assez vite. C'est souvent comme avec un système d'alarme : on agit une fois qu'on a été cambriolé. Or, le problème, quand on est hacké, c'est qu'il arrive que les entreprises ne s'en remettent pas », poursuit Stéphane Vince, directeur du pôle technologie et administration numérique à l'Agence du Numérique (AdN). ■

L.B.

À noter : retrouvez tout le programme de cette cyberweek sur www.digitalwallonia.be/cyberwal/



Un secteur régulièrement visé par des cyberattaques. © E.Gh.

Retrouvez ce reportage en vidéo en scannant le QR Code

Comment rebondir après une cyberattaque ? Le cas du CHRSM

Une cyberattaque est souvent perçue comme un événement lointain. Pourtant, en mai 2023, le Centre Hospitalier Régional Sambre et Meuse (CHRSM), comme de nombreuses institutions publiques, a dû faire face à ce type de menace. En effet, en 2023, environ 93 % des hôpitaux et centres de santé en Belgique ont signalé des failles de sécurité, avec une tendance croissante dans les cyberattaques.

L'institution hospitalière a su réagir rapidement et avec efficience, dans les premières heures. Le PUH (plan d'urgence hospitalière) a été déclenché pour veiller à la continuité des soins et les autorités compétentes telles que l'Autorité de Protection des Données (APD), la police fédérale et la Cyber Emergency Response Team fédérale (CERT) ont été informées. Ces organismes ont accompagné l'hôpital pour tenter d'identifier les responsables et un signalement a été fait.

SE RECONSTRUIRE AVEC RÉSILIENCE

« Nous n'avons pas attendu cette attaque pour intégrer la cybersécurité dans notre plan stratégique », explique Bastien Ducarme, conseiller en sécurité de l'information au CHRSM. « Des audits réguliers avaient déjà révélé des failles potentielles et des améliorations techniques à apporter. Des investissements informatiques étaient en cours de déploiement. Ces mises à jour prennent du temps, car elles doivent respecter des procédures de marché public. Mais cet incident a souligné la pertinence de nos actions et nous a poussés à les accélérer. »

© D.R.

Si le CHRSM a redoublé d'efforts pour renforcer ses systèmes, il s'est conforté également dans l'importance des campagnes de sensibilisation de son personnel à la cybersécurité. « Nous poursuivons la prévention entamée il y a déjà quelques années », confirme Charlotte Decallonne, responsable communication du CHRSM. « Chaque nouvel employé reçoit des consignes claires contre les tentatives de phishing et nous proposons des formations en ligne. Notre force dans cette attaque fut la capacité de réaction de tous et une communication claire vers l'interne comme vers l'externe. »

Le CHRSM, qui a toujours été vigilant, est désormais plus proactif face aux cybermenaces. « Le risque zéro n'existe pas, mais nous avons établi des protocoles d'urgence, comme la possibilité de couper les connexions avec d'autres institutions si nécessaire », précise Jérémy Delforge, adjoint au responsable communication. « La sécurité de nos patients et de notre personnel est au cœur de nos réflexions. Grâce à un monitoring régulier et à des couches de sécurité supplémentaires, nous sommes mieux équipés. Nous travaillons au quotidien afin de protéger nos systèmes tout en restant vigilants face à l'évolution des menaces. » ■