
# Bienvenue

# En attendant Godot…

**Société éditrice :**
Special Partner
**Siège social :**
84 Avenue de la République
75011 Paris
**Directeur de publication :**
Xavier Lebranchu
xavier.lebranchu@dsih.fr
**Rédaction :**
redaction@dsih.fr
**Coordinatrice générale :**
Hassania Ahrad
hassania.ahrad@dsih.fr
**Rédacteurs :**
Pierre Derrouch,
Morgan Bourven,
Damien Dubois.
**Contributeurs :**
Marguerite Brac de La Perrière,
Cédric Cartau,
Michel Dubois,
Xavier Jung,
Omar Yahia.
**Direction artistique :**
Framboise Communication
Paris
**Pour nous contacter :**
Tél. 02 99 46 24 43
contact@dsih.fr
**Abonnement :**
Tél. 02 99 46 24 43
**Courrier :**
84 avenue de la République,
75011 Paris
**Courriel :** abonnement@dsih.fr
**Tarif d'abonnement France :**
3 numéros par an, 64€ TTC
**Étranger :** nous consulter
**CNIL :** 1436001
**INPI :** 113813102
**Dépôt légal :** à parution
**Impression :** Corlet
**Tirage :** 4 500 ex
**ISSN :** 2110-6827
**Périodicité :** Quadrimestrielle
Imprimé en France

Et un de plus ! Cette fois, c'est au tour du Centre hospitalier de Bourg-en-Bresse d'avoir été épinglé au tableau de chasse des hackers, dans la nuit du 10 au 11 avril. Pas une semaine où presque sans apprendre qu'un établissement de santé français s'est fait phagocyter ses données. Vous pouvez même suivre cette mauvaise série sur une carte de l'association Déclic[1].

L'État et ses représentants ont compris les enjeux et mettent les bouchées doubles pour aider les établissements à renforcer l'étanchéité de leurs systèmes d'information. Le dossier de ce numéro 39 vous en donne un aperçu. Hélas, à l'heure de mettre sous presse, nous n'avions pas encore les résultats des premiers travaux de la *task force* cyber lancée fin 2022.

Les progrès restant à accomplir ne sont pas seulement techniques. Dans un article du *Télégramme* du 3 avril dernier, le directeur des systèmes d'information du CHU de Brest, mis lui aussi en coupe réglée début mars, rapporte que l'intrusion aurait pu avoir été orchestrée depuis l'ordinateur portable dépourvu de protection d'un agent qui s'était connecté au réseau de l'établissement. Guillaume Guinguené, Senior Solutions Engineer chez One-Trust, l'un des invités du petit déjeuner organisé fin janvier par *InCyber*, le média de la communauté FIC, le dit autrement : *« Le maillon faible, c'est souvent entre l'écran et la chaise. »* Une faille qui ne se patche pas. Vincent Trély, fondateur de l'Apssis également présent, a proposé une solution piquante : *« Distiller un peu de paranoïa »* chez les utilisateurs ne nuit pas. Et d'ajouter toutefois, compréhensif : *« On ne peut pas faire que les contraindre […]. Il faut réfléchir à leurs exigences métiers. »* De fait, les utilisateurs comprennent mal qu'à l'heure de l'identification par reconnaissance faciale il faille encore recourir à une bonne vieille carte CPS.

Quoi qu'il en soit, le discours sur la nécessité de respecter des bonnes pratiques de sécurité paraît infuser dans les esprits à tous les échelons. Au point même d'en arriver à une situation paradoxale. Patrice Garcia, DSI du Centre hospitalier sud francilien hacké menu en août 2022, a commis un drôle de lapsus lors du 8e Conseil du numérique de santé en décembre dernier. Au lieu de parler d'une gestion de crise réussie, il s'est félicité d'une *« crise réussie »*. Il n'est pas défendu d'y percevoir un peu de fatalisme. Comme si tous les hôpitaux étaient certains de se faire *data hacker* à un moment ou à un autre, et que le seul challenge consisterait désormais à s'en sortir le mieux possible. Il est vrai qu'avec 100 % des processus métiers d'un établissement de santé aujourd'hui numérisés, la surface d'attaque potentielle est large, d'autant que de nombreuses installations comptent quelques heures de vol au compteur. Le crash n'est jamais loin. Et, souligne Guillaume Guinguené, *« il est impossible de sécuriser un hôpital à 100 % »*.

Il faut alors se féliciter de la publication de l'instruction ministérielle SHFDS/FSSI/2023/15 du 30 janvier 2023 relative à l'obligation de réaliser des exercices de crise cyber dans les établissements de santé et… à leur financement. Mais l'argent ne suffit pas. Vincent Trély a eu la bonne idée de souligner la faiblesse du maillage des responsables de la sécurité des systèmes d'information hospitaliers sur le territoire national. La donnée est peu médiatisée : *« En 2023, il y a entre 150 et 180 RSSI dans le secteur de la santé pour 3 000 établissements de santé publics et privés. Ce n'est pas la fête ! »* Pour pallier les carences de moyens, une disposition s'impose à ses yeux : *« Il faut mutualiser partout où cela est possible à l'échelle d'un territoire : gouvernance, achats et exploitation des systèmes d'information… Le pire aujourd'hui serait de dire : "Il y a de l'argent de l'État qui tombe, on va le diviser par le nombre d'hôpitaux…" Chacun fera sa petite acquisition [d'une solution de sécurité] dans son coin sans faire avancer le sujet. »* Ah ! Cyber m'était conté :

– Anne, ma sœur Anne, ne vois-tu rien venir ?
– Je ne vois rien que le ciel qui poudroie…

Et l'herbe qui verdoie, dans le champ de la cybersécurité, est-ce pour bientôt… ?

En attendant Godot, Barbe-Bleue poursuit ses emplettes.

**Bonne lecture**

■ **Pierre Derrouch**

[1] https://www.dpo-partage.fr/carte-declic-des-cyberattaques