LES ENGAGÉS

Un candidat affronte Prévot pour « rajouter l'ADN chrétien »

© D.R.

Il y aura donc au moins un autre candidat à la présidence des Engagés face à Maxime Prévot, le 22 juin prochain. Si celui-ci n'a pas formellement redit qu'il serait candidat à cette élection en bureau politique, lundi matin, le président sortant du CDH a affirmé, depuis des mois, qu'il remettrait son mandat en jeu après l'adoption du nouveau manifeste et des statuts centristes – ce qui fut fait samedi, en congrès. Le député-bourgmestre de Namur remplira donc bien le formulaire de candidature présidentielle (les intéressés ont jusqu'au 27 mai pour le faire).

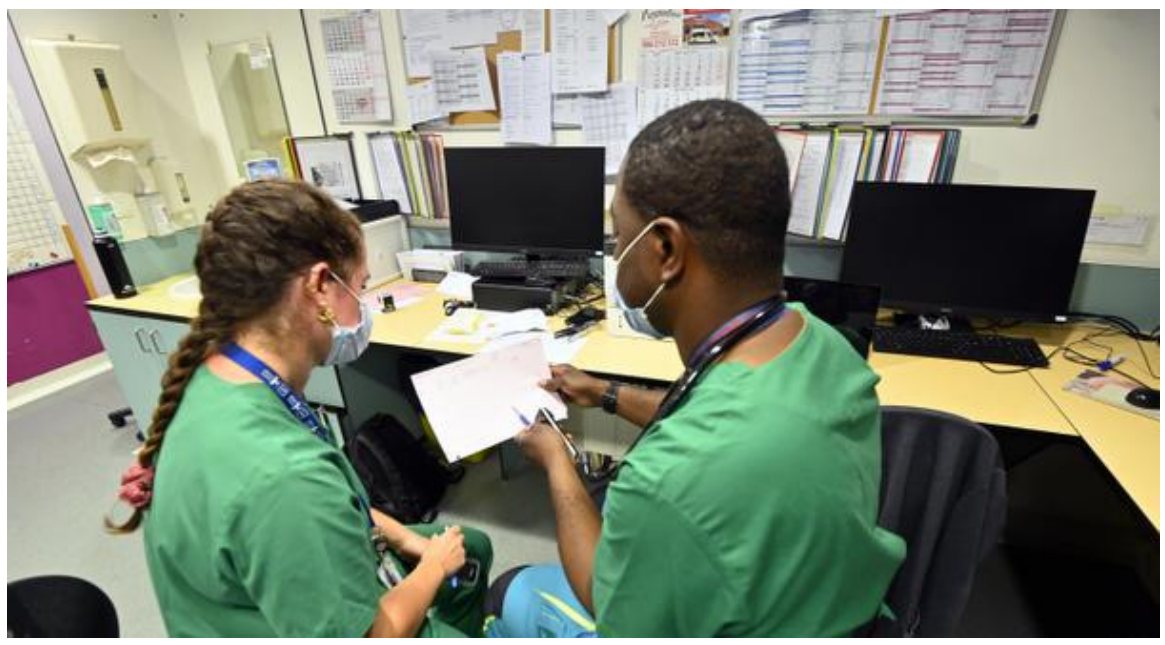
Mais face à lui, un autre centriste s'est déjà profilé : Marc-Antoine Mathijsen, qui veut « réconcilier les chrétiens-démocrates avec les humanistes », lui qui juge son parti « profondément divisé » et assure bénéficier de soutiens non négligeables. Mais il était seul pour annoncer sa candidature lundi après-midi et refusait de dire quoi que ce soit de ses soutiens.

Pour le situer, rappelons qu'après la transformation du PSC en CDH, Marc-Antoine Mathijsen avait quitté le parti pour fonder avec d'autres le CDF (chrétiens-démocrates francophones, dissous en 2013) – « une erreur », dit-il aujourd'hui –, pour ensuite revenir au CDH puis le quitter pour le MR, et revenir au CDH, devenu Les Engagés, qu'il espère donc présider. Tout en étant d'accord avec « 90 % du nouveau manifeste », il déplore en effet que le parti « abandonne toute référence chrétienne, rejette la foi dans la sphère privée, supprime les cours de religion en secondaire ». S'il est élu, il entend « rajouter l'ADN politique issu de la démocratie chrétienne ». Pour lui, Maxime Prévot fait d'ailleurs « du *bashing* anti-chrétien ». Lui veut au contraire « réactualiser la vision idéologique chrétienne pour qu'elle réponde aux défis de la société actuelle ». Et « lier le sort » des Engagés au CD&V, en « renouant un axe fort avec celui-ci ». MA.D.

INFORMATIQUE

Les hôpitaux, cibles de choix des cybercriminels

La dépendance croissante des hôpitaux aux objets connectés et les données médicales qu'ils brassent font d'eux des proies intéressantes pour les hackers mal intentionnés, et plus spécifiquement pour ceux qui opèrent des attaques de type « ransomware ».



ARTHUR SENTE

Consultations annulées, opérations reportées, police dépêchée sur place… L'attaque informatique qui a mis à sac l'armature IT de l'intercommunale Vivalia – laquelle gère 6 hôpitaux et 4 maisons en province de Luxembourg – laisse l'institution groggy. « C'est une faille classique. Il y a eu un vol de mot de passe, puis la personne a essayé de rentrer dans le système jusqu'au moment où elle y est parvenue », prend la peine de résumer Yves-Henri Serckx, directeur informatique de Vivalia, au cœur d'une journée chaotique. Selon ce dernier, l'assaut s'inscrit en point culminant d'une menace en état d'hyperactivité depuis plusieurs mois : « Par exemple, au début du lancement des hostilités en Ukraine, nous avons parfois reçu plus de 8.000 spams par heure. »

Pour l'heure, l'attaque qui a frappé Vivalia n'est pas signée. Et officiellement, aucune demande de rançon n'a été envoyée à la victime. Mais le type d'assaut fait fortement penser à une intrusion de type « ransomware », un mode opératoire qui consiste à pénétrer dans des serveurs, à en extraire des données et à les crypter, puis à réclamer une rançon en échange d'une clé de déchiffrement, voire de la non-divulgation de ces données sur le darkweb.

L'épisode vient ainsi rappeler que les hôpitaux sont des cibles de choix pour les hackers mal intentionnés. En 2021, la Heilige Hartziekenhuis de Mol, la clinique Saint-Luc de Bouge et le Chwapi de Tournai sont autant de victimes qui en ont fait les frais. Si certains « gangs » informatiques spécialisés dans ce type d'attaques affichent publiquement leur volonté de ne pas s'en prendre à des cibles hospitalières, d'autres en ont fait un vrai business. Alors que le Centre hospitalier d'Arles, en France, subissait une agression de ce type l'été dernier, le groupe Vice Society revendiquait ainsi le méfait sur sa plateforme en exposant sa cible au travers d'un message brillant par son cynisme : « Peut-être qu'ils savent comment soigner les gens, mais ils ne savent pas comment protéger leur réseau. Les docteurs de Vice Society ont tout soigné. »

Un électrochoc ?

Geert Baudewijns, CEO de la société de cyberdéfense belge Secutec, observe plusieurs raisons à cet attrait. Il y a notamment le fait que ces infrastructures fonctionnent de plus en plus grâce à ce qu'on appelle « l'internet des objets » et à des machines connectées à leur réseau. « Ces appareils peuvent être rapidement touchés et sont facilement utilisés comme passerelles vers les services informatiques », explique-t-il. Le fait qu'il s'agisse d'infrastructures critiques peut aussi pousser les attaquants à croire qu'elles seront plus enclines à payer une rançon. Enfin, il y a les données médicales et leur potentielle valeur à capter. « La dernière fois que je me suis renseigné », poursuit l'expert informatique, « on parlait de 2,5 dollars par dossier de patient pour des données classiques telles que des adresses, un numéro de téléphone, une adresse mail et un type de problématique médicale lié au patient. Si l'on sait qu'une personne a le diabète, ça sera très utile pour vendre ces données à des sociétés fabriquant des produits amincissants. »

Face à cette menace croissante, la Belgique s'est-elle adaptée ? Yves Smeets, directeur général de la fédération d'institutions hospitalières Santhea, estime que l'électrochoc n'a pas vraiment eu lieu : « Le souci, c'est qu'on n'en discute pas beaucoup. Aujourd'hui, il y a de la coopération spontanée entre institutions pour échanger sur les bonnes pratiques. Mais nous sommes en demande d'une structuration plus officielle. » Selon lui, un des problèmes réside dans le fait que les hôpitaux belges n'ont toujours pas été reconnus comme des opérateurs de services essentiels (OSE) – ce qui leur imposerait des obligations supplémentaires en termes de protection et de déclaration d'incident, mais leur permettrait aussi de bénéficier de financements spécifiques pour assurer leur défense et de rejoindre un réseau européen d'échange d'information.

Au cabinet de Frank Vandenbroucke (Vooruit), on préfère ne pas trop attacher d'importance à cet aspect, plutôt vu comme une charge supplémentaire qui risquerait de peser sur les hôpitaux, mais rappeler qu'outre le fait que ceux-ci font déjà l'objet d'une attention particulière de la part du Centre pour la cybersécurité Belgique, des investissements seront bientôt consentis au travers du Plan de relance belge pour les soutenir sur le plan IT – 20 millions d'euros, prévus pour 2022-2023, viennent d'être approuvés en Conseil des ministres.

« Le souci, c'est qu'on ne discute pas beaucoup de cette menace », regrette Yves Smeets, directeur général de Santhea. © BELGA.