ÉLYSÉE

VISIOCONFÉRENCE AVEC LES CENTRES HOSPITALIERS DE DAX ET DE VILLEFRANCHE-SUR-SAÔNE – PRÉSENTATION DE LA STRATÉGIE NATIONALE POUR LA CYBERSÉCURITÉ.

18 FÉVRIER 2021 - SEUL LE PRONONCÉ FAIT FOI

Merci aux équipes de Dax et de Villefranche-sur-Saône qui ont pris de leur temps, en plus du reste, pour venir témoigner, nous expliquer, nous aider à mieux comprendre. Et merci aux équipes de l'ANSSI, de Orange Cyberdéfense du travail avec les DSI et les équipes sur place pour venir au plus vite essayer de régler ces crises.

Je pense qu'on a pu voir à travers vos témoignages et ces retours d'expérience à quel point ces attaques cyber qui peuvent paraître très abstraites, et c'est vrai qui ne faisaient pas partie du quotidien de notre pays et dont on parlait peu, peuvent en quelques instants venir percuter tout un système d'organisation et, vous l'avez très bien dit, désorganiser l'utilisation d'un dossier médical, empêcher la stérilisation nécessaire aux interventions chirurgicales, ne plus permettre de visualiser les images, au fond, ne plus permettre ce qui est le cœur du travail et nous mettre dans une situation de grande vulnérabilité. Tout cela montre combien cette menace est extrêmement sérieuse, parfois vitale, et touche tous les secteurs.

On a aujourd'hui l'exemple, parce que l'actualité, si je puis dire, nous l'impose et vous en êtes les victimes, des hôpitaux. Le directeur général de l'ANSSI rappelait que c'est 11% des cas que nous avons eu à traiter mais les administrations, les médias, les petites et moyennes entreprises, des grands groupes y compris d'ailleurs dans le numérique, ont été touchés, et même dans le domaine de la sécurité informatique, ont eu à subir durant les derniers mois des attaques cyber.

Et ça touche aussi tous les pays. Il faut être très clair : nous sommes parmi les plus avancés dans la réponse et nous sommes tous en train de découvrir ces nouvelles attaques. Certaines sont étatiques et font partie de la nouvelle conflictualité entre Etats. D'autres attaques sont mafieuses. C'est le cas en ce qui vous concerne. Mais on a vu très clairement aux Etats-Unis en fin 2020 des agences fédérales et des entreprises être attaquées. On a vu l'Agence européenne du médicament être aussi attaquée. Donc les systèmes les plus stratégiques dans tous les pays peuvent faire l'objet de telles attaques avec énormément de désorganisation et avec, soit des motifs cybercriminels, soit des fins lucratives, soit des fins de déstabilisation.

Face à cela, depuis 2017 nous nous sommes organisés. On s'est d'abord donné des moyens. L'ANSSI a procédé à environ 200 recrutements supplémentaires pour permettre, je crois que vos exemples l'ont très bien illustré, à des équipes de se déployer sur site, de faire face, et on va continuer à y travailler, à des attaques multiples et simultanées, ce qui est un risque redoutable pour moi.

On s'est ensuite organisé avec L'appel de Paris pour la confiance et la sécurité dans le cyberespace de novembre 2018 pour essayer de créer cette conscience collective, une culture interétatique sur ce sujet. Et nous avons beaucoup accentué la coopération policière et judiciaire qui ont permis de démanteler des réseaux, d'interpeller des cybercriminels, par exemple le réseau Egregor et plusieurs autres. On va continuer à renforcer cette coopération police/justice, cette coopération entre pays touchés et cette coopération entière entre nos services, d'où la présence du coordinateur également à nos côtés, parce que c'est un élément clé. Et on sait très bien que ça peut être aussi un axe utilisé par nos ennemis, je veux parler d'Etats, mais on peut aussi avoir l'axe cyber qui soit utilisé par des groupements terroristes organisés ou certains de leur proxy.

Au-delà de ces moyens humains et de cette organisation collective dont on s'est dotés, on a aussi, dans le plan de Relance, décidé que la transition numérique serait un axe essentiel. Ça rejoint la discussion qu'on avait avec vos deux hôpitaux. On a placé 7 milliards d'euros directement sur cet enjeu sur le

numérique : un milliard d'euros consacré à la mise à niveau des services publics et 2 milliards dans le Ségur de la santé sur le volet numérique qui doivent permettre une mise à niveau du secteur sanitaire et médico-social. Parce que le paradoxe, c'est qu'au moment où cette menace devient tangible et visible, c'est aussi le moment où nous devons accélérer sur la numérisation de beaucoup de choses. Donc il faut à la fois accélérer pour continuer d'investir, numériser tous les acteurs du public, par exemple, de la santé et du reste de la société parce que c'est un gain de productivité, du bien-être, quelque chose qui nous permettra d'être plus performants et plus innovants. Et il faut dans le même temps, se doter tout de suite de systèmes plus résilients. Donc pour moi, ces investissements du plan de Relance, ces 7 milliards numériques doivent aller vers des systèmes beaucoup plus robustes et testés avec nos acteurs, mais on doit aussi prévoir en même temps les systèmes de défense, d'où ce plan cyber.

On a donc décidé d'accélérer la stratégie nationale pour la cybersécurité à travers le plan qui sera décliné ensuite par le secrétaire d'Etat et plusieurs ministres. On va se doter d'un milliard d'euros, largement dans le cadre du plan de relance et du programme d'investissement d'avenir pour investir sur plusieurs axes. D'abord, apporter un soutien à la recherche et au développement de nouvelles technologies, souveraines, et créer, ce faisant, un écosystème beaucoup plus soudé, plus performant, qui sera réuni dans le campus cyber qui vient nous être présenté et qui donc ouvrira ses portes à l'automne.

Ensuite, soutenir l'adoption de solutions cyber par les petites et moyennes organisations, publiques et privées, avec en particulier les nouveaux moyens dont s'est doté l'ANSSI, mais avec tout ce programme de soutien à l'égard des hôpitaux, des collectivités territoriales ? Et donc avoir une infrastructure et une organisation qui permette d'adopter des solutions cyber, et au fond, de réagir encore plus vite et d'avoir tout de suite des barrières qui se mettent en place quand on est attaqué pour faire référence aux exemples que vous avez cités.

Et puis, l'objectif de ce plan, ça va être aussi de renforcer les formations dans ce domaine, et à horizon 2025, de doubler le nombre d'emplois dans ce secteur stratégique. Car on le voit bien, en ce qui concerne l'ANSSI, les prestataires privés, mais également les DSI qui sont là pour les hôpitaux, et c'est vrai pour les collectivités locales, et demain pour une université ou un laboratoire de recherche d'excellence dans tel ou tel domaine : on a besoin d'avoir des emplois qualifiés dans le domaine cyber qui ont justement ces compétences.

Pour ce qui est, et je finirai sur ce point, pour ce qui est du secteur de la santé et du médico-social, même si ça n'a fait que 11 % des attaques, on est sur le cœur du système, qui plus est au moment d'une pandémie, et on est confronté à un risque vital. C'est votre quotidien à vous et quand ça vous empêche de fonctionner, l'attaque cyber peut avoir des conséquences dramatiques. On a décidé d'accentuer encore les choses. Le ministre des Solidarités et de la Santé et le secrétaire d'État au Numérique préciseront les mesures décidées et je voulais simplement insister sur quelques points.

D'abord, on va mettre en place un observatoire permanent du niveau de sécurité des établissements de santé. Depuis l'attaque contre le CHU de Rouen, il y a un peu plus d'un an, on a beaucoup accentué ce travail. Je crois que maintenant, on est mûrs pour qu'il y ait cet observatoire qui permet justement de coordonner tout le travail, de surveiller les vulnérabilités qui sont identifiées mais aussi de mutualiser les expériences acquises pour avoir partout le meilleur niveau.

Ensuite, ça va être tout un travail de sensibilisation à la cybersécurité qui sera systématiquement intégré dans les cursus de formation. Parce qu'on le voit bien, c'est un élément clé dans des professions qui sont en train de se numériser. Une montée en puissance du Service national de cybersurveillance en santé sera portée par l'Agence du numérique en santé et qui va être accélérée afin de fournir un appui en coordination avec l'ANSSI aux structures de santé en matière de détection de leur vulnérabilité.

Et puis pour chaque programme numérique, les structures de santé seront invitées à consacrer systématiquement 5 à 10 % du budget à la cybersécurité, notamment au maintien en condition de

sécurité des SI dans la durée. Cela rejoint exactement la remarque des deux directeurs qui se sont d'ailleurs exprimés sur ce point. Pour ce faire, on a décidé d'augmenter le budget numérique et le budget cyber : au total, on aura 350 millions d'euros, comme je le disais, des 2 milliards du Ségur de la santé qui sont consacrés au numérique, 350 millions d'euros seront dédiés à renforcer la sécurité des systèmes d'information de santé impliqués dans les échanges de données du parcours de soins. Et on va réévaluer chaque année les besoins puisque je n'exclus pas qu'on soit obligés de réévaluer de manière régulière cet investissement. Mais il est clé pour la sécurité de nos systèmes.

Les cyber-attaquants, de manière très claire, ciblent le maillon le plus vulnérable et s'appuient sur les négligences. Donc en la matière, un tel plan n'a de sens que s'il est exhaustif parce que si on laisse des zones de faiblesse, les attaquants finissent par rentrer dans ces zones de faiblesse et il n'y a pas de petite structure dans une protection contre le cyber. Parce que lorsqu'on crée des points de vulnérabilité, que les réflexes ne sont pas bons, à ce moment-là on ouvre des portes à nouveau.

C'est aussi pour cela qu'au-delà de ces investissements, le sujet de formation et d'acculturation est essentiel parce que les oublis de mise à jour, les mots de passe oubliés, l'ouverture d'un message avec une pièce jointe douteuse, des sujets qu'on a tous vécus et qui font notre quotidien sur lesquels on a tous été négligents, ces sujets-là sont aujourd'hui ceux par lesquels nos attaquants rentrent. Et donc c'est aussi une formation à des gestes du quotidien de tous les personnels parce qu'ils ont chacun en quelque sorte une porte d'entrée dans le système et ils peuvent atteindre, à travers ces négligences, le cœur du système avec les conséquences que vous avez décrites. C'est aussi pour cela que derrière ce plan cyber il y a une vigilance collective, une discipline individuelle qui est absolument clé.

Donc voilà les quelques points sur lesquels je voulais insister pour ma part, au-delà de tout ce qui sera détaillé, produit et qui est le fruit d'un très gros travail. Mais la nation va consentir un investissement important sur ce sujet parce que ce qu'on vient de vivre ces dernières semaines à travers vos deux hôpitaux, à travers aussi beaucoup d'autres cas - et il y a beaucoup d'acteurs qui sont attaqués chaque jour - on ne le sait pas, ce n'est pas public, ils ont peur de le rendre public. Certains acteurs font l'objet de demandes de rançon, donc il y a vraiment une criminalité qui est en train de de s'organiser et qui est parfois un continent caché, parce que les victimes vivent en plus dans la peur de la révélation de l'information. Tout cela exige une mobilisation très forte, ces investissements mais aussi cette organisation.

Donc je vous remercie encore une fois d'avoir pris de votre temps dans une actualité que je sais ô combien chargée pour partager cette expérience que vous avez vécue, et moi je voulais partager quelques-unes de ces convictions et des décisions prises. Donc merci infiniment à toutes et tous, à Dax comme à Villefranche-sur-Saône et merci à toutes celles et ceux qui sont autour de moi à Paris du travail fait pour préparer cette stratégie, et surtout maintenant pour la mettre en œuvre. Merci beaucoup et courage pour tout le reste surtout, on est à vos côtés.