Le Président,
21.04.04

Communication du Président du Conseil régional
à la Séance Plénière
Réunion du 10 Novembre 2021
Direction générale des Services
Feuille de route Cybersécurité 2021-2023 – Faire du Centre-Val de Loire un territoire de confiance numérique

L'évolution croissante des attaques cybercriminelles, de plus en plus organisées et préjudiciables, doit conduire les acteurs publics et privés à engager des actions pour assurer la protection et l'intégrité des données, des objets connectés et des infrastructures numériques. A titre d'illustration, sur la seule année 2018, ce sont plus de 50 000 PME françaises qui ont été victimes de cybercriminalité. L'adaptation à cette nouvelle situation est essentielle pour garantir à la fois la continuité de l'activité économique, comme celle du service public.

Face à cette menace, le territoire doit s'organiser, et la Région Centre-Val de Loire fait le choix de se mobiliser. Elle propose d'associer l'ensemble des acteurs publics et privés (entreprises, écoles, associations, collectivités) autour des enjeux de cybersécurité pour porter un territoire de confiance capable de s'adapter, et de se protéger.
Entre novembre 2021 et décembre 2023, la mise en œuvre de la feuille de route « cybersécurité » va s'appuyer sur les compétences locales pour engager une première réaction collective autour de deux grands types d'actions :

- des actions dites pro-actives, d'une part, afin de permettre aux acteurs locaux d'acquérir et de diffuser la culture de la maîtrise du risque,
- des actions dites réactives, d'autre part, afin de proposer un accompagnement immédiat et opérationnel aux incidents et attaques qui touchent les collectivités, entreprises et associations du Centre-Val de Loire, dans le cadre de la plateforme régionale (CSIRT).

Pour ce qui concerne plus particulièrement les entreprises, le suivi des incidents pour les grandes entreprises et les secteurs sensibles relèvent directement de l'Etat (via l'Agence Nationale de Sécurité des Systèmes d'Information – ANSSI). Afin de compenser l'écart important qui existe désormais entre des grands groupes de plus en plus résilients face aux menaces cybers, et les plus petites entreprises mal adaptées pour y répondre, la Région facilitera l'accompagnement des PME et des associations.

Dans le secteur public, les disparités sont elles aussi flagrantes au sein des 1 757 communes de la région. Si les collectivités de taille supérieure disposent de plus de ressources et de compétences pour sécuriser leurs systèmes d'information, les plus petites n'ont souvent pas d'équipe dédiée à l'informatique et sont considérablement fragilisées face à la menace cyber. La continuité du service public nécessite d'engager avec ces collectivités un travail qui leur permette de bénéficier de mutualisation et de solution concrète pour maîtriser le risque cyber.

La Région s'engage à mettre en œuvre la feuille de route « Cybersécurité » durant les 24 mois à venir, en lien avec les acteurs régionaux, à travers trois axes :

- animer l'écosystème « Cybersécurité » en Centre-Val de Loire, et répondre aux besoins de la filière ;
- accompagner les entreprises, les collectivités territoriales et les associations régionales mais aussi les particuliers pour les aider à se prémunir contre les risques Cyber ;
- soutenir l'innovation, la recherche et la formation pour accompagner la transition vers un territoire cyber résilient.

Plus généralement, les enjeux de la cybersécurité rejoignent ceux de la transformation numérique en cours auprès de toutes les catégories de notre population et de tous les secteurs d'activité. Au même titre que l'illectronisme, la médiation numérique, l'accès aux réseaux de communication électronique, ou l'intelligence artificielle, la cybersécurité nous rappelle la nécessité de composer un territoire régional capable d'inclusion et d'humanité. La transformation numérique n'a de limite que dans la confiance et la résilience qu'on lui donne.

I – UNE FEUILLE DE ROUTE DECLINÉE EN 10 ACTIONS CONCRÈTES POUR LES DEUX PROCHAINES ANNÉES

1. Animer et fédérer les initiatives afin de créer un écosystème cyber en Centre-Val de Loire

Action 1 : Créer une gouvernance partagée

Il s'agit de créer un **comité régional d'orientation cyber,** en lien avec DEV'UP, regroupant notamment des représentants des entreprises, des entreprises de services numériques (ESN), des universités, des organismes de formation, de la Gendarmerie nationale, des laboratoires de recherche, des startups via l'association Digital Loire Valley, des représentants des collectivités et des services de l'Etat. Son rôle est de proposer un espace de dialogue entre acteurs, d'une part, et un outil de gouvernance stratégique et de coordination des actions, d'autre part. La Région propose de coanimer la présente feuille de route avec ce comité régional dont le périmètre sera volontairement restreint, afin de lui permettre un fonctionnement agile.

Action 2 : Développer un portail régional cybersécurité

Le portail régional doit permettre de recenser et de cartographier les acteurs, les offres de produits et les services de Cybersécurité en région Centre-Val de Loire. En outre, le lancement d'un premier appel à manifestation d'intérêt (AMI) permettra d'identifier les offreurs de services locaux en matière de cybersécurité, notamment dans le domaine de la remédiation.

Ces offreurs de services pourront ensuite être mis plus facilement en relation auprès des entreprises, des collectivités et des associations de la région. Il est essentiel que l'ensemble de l'offre en matière de cybersécurité soit visible afin d'être connue et utilisée.

Action 3 : Accompagner la montée en compétence des entreprises régionales

La Région relaiera le label « Expert Cyber » porté par l'ANSSI auprès des entreprises. Ce label est destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients.

Action 4 : Organiser les premières assises régionales de la cybersécurité dans le cadre des Human Tech Days 2022

La Région organisera en lien avec DEV'UP et le GIP RECIA, une rencontre annuelle autour des enjeux liés à la cybersécurité dans les entreprises et les collectivités locales.

2. Le parcours cybersécurité pour tous en Centre-Val de Loire : Accompagner et sensibiliser les entreprises, les collectivités, les associations

Action 5 : Créer et mettre en œuvre une plateforme de réponse de premier niveau pour les entreprises, les collectivités territoriales et les associations

La plateforme régionale d'appui doit accompagner les entreprises, collectivités et associations victimes de cyber-attaques, par le traitement des incidents de cybersécurité.

Cette plateforme téléphonique constitue le cœur de la réponse régionale aux incidents de cybersécurité par la fédération et l'animation des acteurs publics et privés. Elle sera menée en partenariat avec l'Etat, l'ANSSI, Dev'UP (pour les entreprises) et le GIP RECIA (pour les collectivités et les associations).

Les missions du CSIRT (traduction du terme anglais de *Computer Security Incident Response Team*) sont de :

- Proposer un service de réponse téléphonique de 1er niveau aux entreprises, collectivités et associations.
- Qualifier les incidents et transmettre les premiers bons réflexes aux bénéficiaires.
- Centraliser les déclarations d'incidents cyber (tout dysfonctionnement d'un système d'information avec une origine malveillante).
- Mettre en relation l'entité victime avec les organisations en charge de l'accompagner dans la résolution de l'incident : prestataires de réponse à incident en charge d'analyser la situation et de restaurer le système d'information ; services de police et de gendarmerie en charge du traitement judiciaire de l'incident.
- Sensibiliser et former les bénéficiaires, partager les bonnes pratiques de cybersécurité.
- Être le pivot régional des échanges cyber entre les autres CSIRT, les bénéficiaires, les services judiciaires, les prestataires de réponses aux incidents.
- Les agents seront formés par l'ANSSI dans le cadre d'un plan de formation national.

Une articulation et une mutualisation seront construites entre cette plateforme et les initiatives portées par le GIP E-Santé Centre afin de pouvoir accompagner les établissements de santé mais aussi les établissements du secteur médico-social (ex : EPHAD), sujets à des attaques cybers de plus en plus nombreuses.

Action 6 : Construire et proposer un catalogue de service au bénéfice des entreprises et organismes publics

Pour un trop grand nombre d'entreprises encore, les enjeux induits par la digitalisation sont sous-estimés, les bonnes pratiques liées à la cybersécurité demeurent méconnues et l'intégration d'une culture numérique fait l'objet de fortes réticences.

Il s'agit d'élaborer un cadre d'intervention proposant des diagnostics et des audits de premier niveau en matière de sécurité informatique. Pour les entreprises, le programme pourrait s'appuyer sur le dispositif "Cap Conseil" déjà proposé par la Région. Pour les Collectivités, le GIP RECIA pourra étoffer son offre actuelle à travers un dispositif alliant diagnostic, préconisation et mise en œuvre des investissements cyber. Au terme de la feuille de route, l'objectif est de proposer un catalogue d'offres de services adaptés aux besoins des collectivités et des entreprises.

Action 7 : Sensibiliser le grand public et notamment les jeunes

Chaque fois que quelqu'un utilise un logiciel, visite un site Internet, ouvre un mail ou encore utilise un objet connecté, il peut potentiellement se retrouver face à un risque d'attaque cyber. Le grand public doit en prendre conscience. La Région propose de constituer un dispositif de sensibilisation du grand public face à ces enjeux de cybersécurité et de diffusion des bonnes pratiques en matière numérique.

Ce programme régional de sensibilisation/formation à destination du grand public associerait notamment la Gendarmerie nationale, et se déploierait en s'appuyant sur le réseau des tiers-lieux régionaux, des espaces publics numériques – notamment via le Hub de médiation numérique (Hub-LO) – mais aussi sur la plateforme Yep's. Ce projet pourrait également accompagner les initiatives citoyennes, y compris internationales, dans le cadre d'appel à projet spécifique. L'Education nationale pourra également être mobilisées dans le cadre des apprentissage (NSI-SNT dans le cadre du parcours en Lycée).

3. Soutenir la formation, l'innovation, et la recherche en Cybersécurité

Action 8 : Soutenir la mobilisation des acteurs de la recherche et de l'innovation autour des enjeux de cybersécurité

Cette mobilisation passera par le lancement dès 2022 d'un appel à manifestation d'intérêt pour la création d'un « campus régional Cyber », en lien avec l'ensemble des acteurs de la filière. L'objectif de cet appel est de pouvoir identifier les initiatives locales et de mobiliser les ressources régionales pour favoriser un passage à l'échelle régionale, et ainsi apporter une réponse à la pénurie de talents. La mobilisation passera également par les universités et les écoles qui proposent et proposeront des formations diplômantes en cybersécurité sur les aspects technologiques, éthiques, juridiques, d'intelligence économique et de management du cyber-risque, la Région favorisera la labellisation de l'offre de formation enseignement supérieur en RCVL (SecNum Edu).

La Région affichera son soutien à la thématique cybersécurité dans ses appels à projets recherche.

Action 9 : Identifier et répondre aux besoins de formation en cybersécurité

A long terme, la formation est essentielle pour organiser et sécuriser le territoire en matière de cybersécurité. Dès 2022, la Région va lancer un recensement et une cartographie des acteurs et des compétences territorialisées pour objectiver la situation et le positionnement régional sur le sujet.

Cette étude est essentielle pour permettre d'identifier les entreprises en capacité de répondre à ces enjeux, et celles qui nécessitent une montée en compétence.

Dans le même temps, elle organisera une expression des besoins de formation et de recrutement avec les entreprises du secteur afin d'envisager des modules de formation complémentaires à l'offre numérique de droit commun, voire la création d'une offre spécifique "Cyber" dans le cadre d'un Défi (développement de l'emploi par des formations inclusives) à destination des personnes en recherche d'emploi (PRF – Programme régional de formation).

Pour rappel et de façon complémentaire, la Région soutient la création du Campus des Métiers et des Qualifications (CMQ) "Transformation Numérique". Ce campus a vocation à promouvoir et coordonner les actions des acteurs économiques, de l'innovation, de la formation, de l'orientation et de l'insertion professionnelle dans le secteur numérique. Il permet d'identifier les besoins des entreprises en matière de nouvelles compétences et de nouveaux métiers, et tout particulièrement en cybersécurité. Il va permettre de construire des formations tout au long de la vie adaptées aux besoins de ce secteur.

Il s'agit notamment de développer des formations en cyber dans le second degré et dans l'enseignement supérieur (BTS, notamment), et ce dans la continuité de la Stratégie nationale de lutte contre la cybercriminalité, mais aussi de proposer des modules d'enseignement "cyber" dès le lycée.

La Région sollicitera l'Etat pour ouvrir de nouvelles formations notamment de Diplôme Universitaire (DU), avec l'ambition d'une mise en application dès la rentrée 2022.

Action 10 : Sécuriser les services du Conseil régional et des lycées

Cette action vise notamment le renforcement et la sécurisation des réseaux tant au siège que dans les lycées. Partant du constat que 90 % des cyberattaques ont comme point d'entrée les adresses emails, un dispositif de sensibilisation aux risques d'hameçonnage a été déployé depuis cet été à destination des utilisateurs des services numériques (élus et agents).

Dans le cadre du volet cybersécurité de France Relance, le Conseil régional s'est engagé dans le parcours cybersécurité proposé et financé par l'ANSSI. Piloté par le Responsable Sécurité des Systèmes d'Information (RSSI) du Conseil Régional, il vise à effectuer un état des lieux, définir un plan de sécurisation et mettre en œuvre les mesures pour corriger les vulnérabilités qui pourraient être identifiées.

Dans le contexte des lycées, la responsabilité de la sécurité du système d'Information est de la compétence de l'Etat. Le RSSI du Rectorat communique vers le Service Numérique Éducatif la politique à mettre en œuvre et la collectivité la mets en application. Ce partenariat fort permet d'accompagner, former nos utilisateurs (élèves, enseignants, personnels de direction, agents région) et de renforcer la sécurité que l'on doit mettre en place avec un public essentiellement mineur.

II - **PROPOSITIONS DU PRESIDENT**

Je vous propose d'adopter la délibération suivante :

L'Assemblée Plénière, réunie le 10 novembre 2021, décide :

- De prendre connaissance de la communication

François BONNEAU