Garantir la sécurité de tout un ensemble d'échanges numériques est une condition nécessaire pour que l'ensemble des usagers, entreprises, administrations publiques, associations et particuliers se sentent en confiance dans leurs pratiques numériques et puissent ainsi les exercer librement et donc les développer.

Cette confiance passe par des actions que chacun des acteurs doit mettre en place pour garantir sa propre sécurité et celle de ceux qui sont en relation avec lui.

La surface d'exposition aux risques est croissante compte tenu de l'augmentation du nombre d'utilisateurs et des objets connectés, et la professionnalisation des fraudeurs. La cybersécurité relève de la sphère économique comme de la sphère politique car elle pose également des questions de souveraineté. Des actions ont été mises en œuvre au plan national et au plan régional.

La Cybersécurité est également un marché en pleine croissance pour lequel des opportunités existent et les acteurs régionaux ne sont pas dépourvus d'atouts en la matière. Pour renforcer et développer la cybersécurité en Auvergne-Rhône-Alpes, territoire qui a fait du développement numérique une de ses priorités, le CESER propose aux acteurs régionaux trois axes d'actions : la sensibilisation-formation, notamment des plus jeunes, l'accompagnement des petites structures économiques, publics et associatives dans la mise en œuvre de couverture aux risques, et la réunion des initiatives sous une bannière commune pour y donner davantage de lisibilité.

Face à ce nouveau défi qu'est la cybersécurité des réponses sont à construire, à inventer pour faire face à des actes malveillants qui évoluent très vite : leur pertinence sera la garantie de la confiance qui sera accordée aux actes numériques et donc à la liberté d'usage qui en découle.

7 entreprises sur 10
ont été **victimes d'**(au moins)
1 tentative de fraude
sur l'année écoulée

1 entreprise sur 3
a subi
au moins 1 fraude avérée
en 2017

2/3 des mails
sont
des spams

8 à 10 % des spams
sont considérés comme
des produits malveillants

Télécharger la contribution
www.auvergnerhonealpes.fr/ceser

Crédit photos : 123 RF
istockphoto

CESER Auvergne - Rhône-Alpes / Lyon
8 rue Paul Montrochet – CS 90051 – 69285 Lyon cedex 02
T. 04 26 73 49 73 – F. 04 26 73 51 98

CESER Auvergne - Rhône-Alpes / Clermont-Ferrand
59 Bd Léon Jouhaux – CS 90706 - 63050 Clermont-Ferrand Cedex 2
T. 04.73.29.45.29 – F. 04.73.29.45.20

Janvier 2019

CYBERSÉCURITE : UNE URGENCE À SE PROTEGER

Captation d'informations sur la vie privée, surveillance des sites visités, intégrité des données stockées, prise de contrôle ou altération des systèmes d'information, détournement de flux financiers, piratage de messagerie, de comptes, usurpation d'identités, tels sont les grands enjeux de la sécurité du numérique.
Préoccupation relativement récente, la cybersécurité doit répondre à différents enjeux et prémunir de certains risques. La presse se fait l'écho d'un certain nombre de cyberattaques particulièrement marquantes.

Objectifs

Il s'agit d'attirer l'attention des acteurs régionaux sur ce sujet. Il concerne l'ensemble des organisations : entreprises, associations collectivités et acteurs publics. Il concerne également les citoyens. Ils ne sont pas à l'abri de certaines attaques directement ou indirectement par les liens qu'ils entretiennent avec ces entités.

Enjeux

Une surface d'exposition aux risques est croissante, compte tenu de l'augmentation, d'une part, des utilisateurs et des objets connectés, et de la diversité des cyberattaquants d'autre part.
La cybersécurité est la responsabilité de tous. Chaque objet connecté donc chaque utilisateur peut être le point d'entrée d'une cyberattaque. La sécurité est tout autant menacée par la professionnalisation des attaquants potentiels que par l'absence de protection élémentaire et de négligence qui peuvent être sources de difficultés majeures. Comme dans le domaine sanitaire, pour éviter la propagation de virus, des réflexes de base d'« hygiène numérique » doivent être acquis.
La cybersécurité et son développement sont aussi sources d'opportunités pour le développement de solutions adaptées dont le potentiel économique est très important.
Les enjeux économiques s'entrecroisent avec des enjeux de nature politique, liés à la souveraineté nationale voir européenne.
Un certain nombre de réponses existantes au niveau national ou régional qui sont apportées aux acteurs pour faire face à ce risque.

Démarche

Le CESER pointe quelques recommandations à destination des acteurs régionaux afin de mobiliser davantage et plus rapidement sur ce thème. Il s'agit aussi bien de se prémunir de cette nouvelle forme de délinquance que d'initier des solutions spécifiques en lien avec les particularités économiques du territoire régional. Il s'agit de proposer des pistes afin qu'une région comme Auvergne-Rhône-Alpes qui revendique une position et des atouts dans le secteur du numérique, puisse contribuer à cette problématique.

« Si vous pensez que la technologie peut résoudre vos problèmes de sécurité alors vous n'avez rien compris aux problèmes ni à la technologie ».

Bruce SCHNEIER,
Cryptologue, Spécialiste en sécurité informatique et écrivain américain

CESER Auvergne-Rhône-Alpes
Conseil Économique, Social & Environnemental Régional

AXE 1

Poursuivre et accentuer la sensibilisation des organisations et des particuliers, notamment les plus jeunes

Le risque cyber est récent, à l'inverse d'autres risques, il ne fait pas l'objet, sauf exception, d'une transmission dans les familles, dans les organisations, aussi il convient d'organiser l'information à travers des démarches proactives.

1 **Le CESER propose de mettre en place des exercices de cybersécurité « proches » d'une attaque réelle** (sur le modèle d'un exercice évacuation-incendie). Un logiciel de simulation pourrait être produit par les acteurs de la filière sous l'impulsion notamment du Conseil Régional à destination des organisations, voire des particuliers pour les sensibiliser en situation « réelle ».

2 Concernant les jeunes, **une sensibilisation-formation à la cybersécurité et au traitement des informations (Fake-News) au titre de l'instruction civique pourrait être mise en place**, puis au collège une formation spécifique sur la cybersécurité pourrait être intégré au B2I (Brevet informatique et internet) ou le compléter. **Plus largement à chaque niveau pédagogique des temps consacrés à ce sujet et à ces évolutions très rapides pourraient intégrer les cursus pédagogiques**. Dans la formation des futurs chefs d'entreprise, introduire un temps consacré à ce sujet et notamment leur faire connaître les réponses existantes serait pertinent. Ces démarches pourraient être menées par la Région en collaboration avec les acteurs concernés : rectorats, chambres consulaires ...

3 **La Région et ses partenaires privilégiés comme les quatre moteurs pourraient prendre une initiative à l'échelle européenne sur ce thème (livre blanc, manifeste.) pour inciter à une coopération renforcée**. Une obligation d'information par les fournisseurs d'accès à Internet sur les attaques identifiées pourrait par exemple être suggérée.

4 Dans cette phase de sensibilisation, la société civile doit prendre sa part. **La sensibilisation des citoyens passe également par le relai des organisations représentant la société civile. La société civile peut aussi agir dans la mobilisation pour une politique européenne plus affirmée sur le sujet.** Le CESE européen pourrait se faire l'écho des attentes de la société civile européenne en la matière auprès du parlement européen.

AXE 2

Accompagner les organisations publiques, privées et associatives à se saisir de la question en portant une attention particulière aux petites structures qui sont souvent démunies face à ce défi

Les petites structures sont souvent les plus démunies face au défi de la cybersécurité. Ce thème doit être appréhendé de manière systémique. La sécurité est une chaîne qui concerne tous les acteurs. Une action volontariste de la collectivité régionale appuyée sur sa compétence en matière de développement économique et territorial serait pertinente. Certaines entités à l'échelon régional ont mis en place des plans spécifiques : grandes entreprises, collectivités et associations de taille importante. La Région pourrait s'appuyer sur celles-ci pour promouvoir un programme ambitieux sur ce sujet. Il s'agit notamment de prendre la question sous deux angles.

5 **Un déploiement progressif mais rapide de plans d'actions au niveau des différentes organisations.**

Les têtes de réseau pourraient être mobilisées :

- Consulaires, organisations professionnelles pour les entreprises. Les grands donneurs d'ordre pourraient notamment davantage accompagner les entreprises sous-traitantes dans cette démarche, ils y ont intérêt si l'on considère les liens numériques entre elles dans les processus de production. La fraude aux fournisseurs est un bon exemple de liens exploités par les cyberdélinquants,
- La Région et les grandes collectivités (métropoles, départements) dans l'appui aux petites collectivités,
- Les têtes de réseau associatives pour les associations.

6 **Un numéro vert, dont la Région pourrait assurer la maîtrise d'ouvrage, pour répondre aux situations d'urgence pourrait être expérimenté sur le territoire régional afin d'éviter la propagation de certaines attaques.** Cela pourrait se faire en lien étroit avec les forces de police dont les moyens sont limités sur cette thématique.

AXE 3

Fédérer les acteurs de la cybersécurité régionale et engager des coopérations à l'échelle nationale et européenne

Le marché de la cybersécurité est un marché économique très porteur, des enjeux de souveraineté numérique y sont liés. Les enjeux de constitution d'une filière de la cybersécurité dépassent le strict cadre régional et s'inscrivent davantage dans des perspectives nationales et surtout européennes.
L'articulation de réponses en lien avec le développement de l'intelligence artificielle est déterminante.
Des initiatives en Région ont été lancées ou sont en cours de mise en œuvre. On peut citer le campus numérique, le cluster ECC4IU, le Grenoble Alpes Cyber Security Institute et l'existence de start-up largement identifiées sur ce thème mais aussi un écosystème de recherche et d'innovation particulièrement riches sur ces thématiques.
Sur ces sujets, le tissu industriel d'Auvergne-Rhône-Alpes constitue un terrain d'expérimentation particulièrement pertinent pour valoriser une démarche autour de la protection des systèmes industriels.

7 Le CESER propose que la **Région fédère l'ensemble des initiatives sous une bannière commune, en organisant par exemple une journée rassemblant l'ensemble des acteurs régionaux concernés.**

Elle pourrait notamment aussi inciter de grands acteurs du numérique en Région, tel Google par le biais des ateliers numériques initiés à Saint-Etienne, à engager également une action sur le thème de la cybersécurité. Parallèlement, des coopérations avec des régions ayant développées ces thématiques comme la Bretagne ou Région SUD Alpes Côte d'Azur pourront être mises en œuvre La cybersécurité liée à l'internet des objets est un thème particulièrement porteur pour les régions industrielles comme Auvergne-Rhône-Alpes.

Cet axe est complémentaire par ailleurs de la cybersécurité plus strictement orientée vers les réseaux informatiques qu'ont développé d'autres régions.