Cybersécurité : une mobilisation régionale au service de la sécurité économique des entreprises

La diffusion rapide des technologies numériques et la multiplication des champs d'application du traitement des données constituent autant d'opportunités de développement pour les entreprises. Toutefois, ces opportunités ont leur revers et le risque lié au piratage informatique va grandissant. La protection des entreprises et des organisations est devenue depuis quelques années un enjeu incontournable du développement économique des territoires. Au niveau national comme au niveau régional, des dispositifs structurants ont été mis en œuvre pour fédérer les acteurs économiques autour de la prévention des risques cyber. Dans ce contexte, les systèmes éducatifs et de formation devront jouer un rôle déterminant pour sensibiliser d'une part, former d'autre part les futurs professionnels aux métiers de la cybersécurité.

UNE EXPLOSION DES CYBERATTAQUES, MULTIPLIÉES PAR QUATRE EN UN AN

Sujet vaste et transversal, la cybersécurité est un défi majeur, de plus en plus stratégique et structurant pour toutes les organisations : aucun secteur et aucune activité ne sont épargnés. En ce sens le cyber risque est à concevoir comme faisant partie de la chaîne des risques systémiques (climatique, industriel, terroriste, social, économique, financier, technologique, naturel).

Avec le développement constant des technologies numériques, les surfaces d'exposition aux risques augmentent au sein des organisations, privées comme publiques, en les rendant plus vulnérables aux attaques cyber. Les environnements numériques des entreprises sont, en effet, de plus en plus complexes et fragmentés, passant de petits réseaux sur site, dotés de quelques pare-feux, à une masse de réseaux hybrides, mélangeant systèmes à grande échelle, multi-cloud, objets connectés (IoT - Internet des objets) et systèmes industriels.

En cette période de crises sanitaire et économique, les menaces cyber se sont multipliées. Les attaquants visent désormais les cibles les plus faciles à atteindre, à savoir les TPE / PME / ETI, les collectivités territoriales et les établissements de soin : + 50 % d'attaques ciblant les collectivités en 2020, + 25 % pour les entreprises. Le rapport d'activité 2020 de l'Agence nationale de la sécurité des systèmes d'information (Anssi) constate une explosion des *ransomwares*[1] (ou rançongiciels) dont les signalements ont été multipliés par quatre en un an.

Déjà, la dernière décennie a vu l'Europe et les Etats membres multiplier les initiatives pour structurer les plans en faveur de la cybersécurité et renforcer leur cohésion, notamment via la transposition de la directive NISS[2] sur la cybersécurité des réseaux informatiques. Dès 2016, elle s'est traduite en France par

La mise en œuvre de la cybersécurité comprend trois phases, qui se répètent pour former un cycle :

. la phase amont de maîtrise du risque (analyse de risque, conception, protection, parfois qualification, etc.)
. la phase d'opération (détection, supervision)
. la phase de remédiation (maintien en condition de sécurité avec les mises à jour, restauration, réponse à incident, etc.).

l'identification de 300 entreprises qualifiées d'opérateurs d'importance vitale (OIV) devant justifier un niveau de cybersécurité particulièrement exigeant sous le contrôle de l'Anssi. Cette initiative est actuellement en cours d'extension à l'échelle européenne aux opérateurs de services essentiels (OSE) dont le rôle est primordial au bon fonctionnement de l'économie ou de la société. En France, plusieurs milliers d'OSE ont ainsi été identifiés. L'Anssi vient ainsi de désigner OSE une centaine d'hôpitaux, les amenant à respecter un certain nombre de normes contenues dans la directive NISS.

Par ailleurs, la prise de conscience des risques cyber s'est accélérée depuis 2018 avec l'application du règlement pour la protection des données personnelles (RGPD) visant à assurer la sécurité des données des entreprises, des administrations et des citoyens.

[1] Logiciel chiffrant les données se trouvant dans un système d'information, en vue d'une demande de rançon pour leur déchiffrement, payable en bitcoins et donc impossible à annuler une fois payée
[2] La directive « Network and Information System Security » (NISS) adoptée par l'Europe le 6 juillet 2016 poursuit l'objectif majeur d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information dans l'Union européenne.

UNE STRATÉGIE NATIONALE D'UN MILLIARD D'EUROS

La cybersécurité est désormais pleinement identifiée comme un enjeu clé tant au niveau sociétal qu'économique. Elle est devenue une priorité nationale, comme l'a rappelé le président de la République lors de la présentation de la Stratégie nationale pour la cybersécurité, le 18 février dernier. Doté d'un budget d'un milliard d'euros, ce plan s'articule autour de cinq axes :

- le développement de solutions souveraines de cybersécurité
- le renforcement des liens et des synergies entre acteurs de la filière
- le soutien à l'adoption de solutions cyber, par les individus, les entreprises les collectivités et l'Etat
- la formation des jeunes et des professionnels aux métiers de la cybersécurité
- le soutien en fonds propres aux acteurs de la filière.

Le plan du gouvernement prévoit également d'allouer 136 millions d'euros issus du plan de relance à un volet « cybersécurisation » des territoires, piloté par l'Anssi.

Cette nouvelle stratégie nationale dédiée à la cybersécurité a aussi pour objectif de faire émerger des champions français de la cybersécurité. D'autant que la menace cyber s'amplifie et évolue : en volumétrie, en gravité, en probabilité, en fréquence, en imprévisibilité et surtout en sophistication de stratégie d'attaque, avec des conséquences territoriales préjudiciables, voire irréversibles, sur l'économie et sur l'emploi. Et rares sont les organisations qui dépassent l'angle de vue purement technologique, généralement privilégié dans la réponse aux cybermenaces, pour déployer une stratégie globale intégrant la cyber-résilience.

Il s'avère aussi que la cybersécurité est encore davantage perçue comme un coût que comme un investissement. Or la posture de cybersécurité est dynamique, elle n'est jamais atteinte une fois pour toutes. La méconnaissance de la problématique cyber et la non-perception des risques constituent l'écueil principal. Comme pour les « démarches qualité », si une entreprise n'a pas recours aux modes d'action de la cybersécurité, cela ne peut que lui être fortement dommageable.

En outre, le niveau de cybersécurité de toute entreprise a des conséquences sur son écosystème : autres entreprises, organisations, parties prenantes, clients et consommateurs. On peut à cet égard parler d'« empreinte cyber » de l'entreprise comme on le fait pour l'environnement et le social.

Enfin, la présence à la fois d'un écosystème et d'une culture favorisant la cybersécurité sur un territoire constitue un atout majeur pour son développement, sa compétitivité et son attractivité économiques. D'autant plus que les notions de « territoire de confiance » et d'« entreprises de confiance », alliées à celle de « territoire numérique », s'avèrent de plus en plus prégnantes et discriminantes, en particulier pour les entreprises qui y sont localisées ou celles susceptibles de s'y implanter.

La cybersécurité constitue l'une des composantes essentielles de la sécurité économique, l'un des trois piliers de l'intelligence économique territoriale (IET). Démarche s'appuyant sur une approche interdisciplinaire, l'intelligence économique articule des modes opératoires, combinés et dynamiques, visant à « anticiper », à « influencer » et à « se protéger ».

UNE CHARTE RÉGIONALE « CYBERSÉCURITÉ » POUR PROTÉGER LES ENTREPRISES NORMANDES

En Normandie, sur un panel de 2 000 entreprises interrogées par l'Observatoire des transformations numériques, piloté par la Région, 23,4 % des entreprises ont déjà été confrontées à un piratage ou un risque de cyberattaque.

Les grands secteurs économiques « stratégiques » pour le territoire (biomédical-santé-pharmacie, aéronautique et spatial, automobile, énergie, logistique-portuaire...) ont l'impérieuse nécessité de se protéger des cyberattaques.

Depuis 2017, la Région Normandie est engagée dans un partenariat étroit avec l'Etat sur l'IET qui intègre un volet sécurité/cybersécurité. Cette démarche est conforme à l'esprit de la charte partenariale Etat-Régions de France « Intelligence économique territoriale / sécurité économique » signée le 18 décembre 2019.

Par ailleurs, en lien avec sa Stratégie numérique, la Région a, depuis 2018, la volonté de faire de la cybersécurité un axe fort pour accompagner la transformation numérique des acteurs du territoire. En partenariat avec la chambre de commerce et d'industrie (CCI) de Normandie et avec le soutien de l'Anssi, elle a ainsi notamment permis le déploiement, à l'échelle de la région, d'une charte d'engagement collaboratif pour les prestataires informatiques et numériques normands. Cette charte invite les signataires à respecter les bonnes pratiques en matière de cybersécurité selon les recommandations de l'Anssi et de la Commission nationale informatique et libertés (Cnil). Ils se doivent d'informer, conseiller et inciter leurs clients à adopter de bonnes pratiques numériques. La charte régionale cybersécurité a constitué la première étape d'une dynamique régionale en la matière.

CYBERSÉCURITÉ : DE NOUVELLES COMPÉTENCES À DÉVELOPPER

Une fois sensibilisées au risque cyber, les entreprises cherchent à intégrer et développer en interne une expertise cybersécurité et/ou recourir à des prestataires ou fournisseurs externes. Les défis auxquels elles sont confrontées alors tournent autour de la pénurie de compétences permettant de faire face au volume croissant de menaces sophistiquées. On estime qu'il manque par exemple encore plus de trois millions d'experts en cybersécurité à l'échelle mondiale. En France, ce ne sont pas moins de 8 500 offres d'emplois qui sont non pourvues dans ce secteur. La cybersécurité est un secteur en pleine croissance qui manque cruellement de travailleurs qualifiés.

Que ce soit *via* le Cloud, les applications mobiles, les appareils connectés ou d'autres types de technologies, la transition numérique permet aux entreprises d'accélérer leur développement plus rapidement qu'elles ne peuvent recruter de spécialistes pour protéger leurs infrastructures.

Compte tenu de la rareté des compétences, le développement de formations spécialisées (de niveau BTS, licence pro ou master) permettrait de bénéficier des ressources humaines nécessaires sur les court et moyen termes. Les spécialistes en cybersécurité sont, en effet, des perles rares. Et ces profils sont d'autant plus difficiles à identifier que le champ des missions et compétences de la cybersécurité est vaste, complexe, hétérogène et donc difficile à appréhender pour qui n'y est pas familier.

Dans ce contexte, la formation (et le recrutement) constitue un enjeu fondamental. Aujourd'hui, faute de connaissance de spécificités du domaine, les services en charge des ressources humaines peinent parfois à identifier les profils capables de répondre aux besoins de leur organisation. Néanmoins, mettre en place des formations de niveau bac +2 délivrant une expertise rapidement opérationnelle répondrait déjà à un grand nombre de besoins.

Contrairement aux générations précédentes, les étudiants d'aujourd'hui sont des *digital natives* qui ont grandi avec les nouvelles technologies. Leur dépendance vis-à-vis d'Internet met en exergue la nécessité d'acquérir des compétences en matière de cybersécurité, tant au niveau personnel que professionnel. Les talents de demain devront maîtriser l'architecture, l'administration et la gestion des systèmes d'exploitation, ainsi qu'adopter une vision d'ensemble pour saisir les enjeux liés aux données des entreprises, à leur stockage, exploitation et valorisation.

Il s'agit bien d'éveiller l'intérêt des filles et des garçons dès le collège, et de leur montrer que les métiers de la cybersécurité sont aussi utiles que ceux des pompiers ou des infirmiers pour protéger les populations. Avec de nouvelles représentations à construire.

L'Anssi a mis en place des dispositifs pour impulser, encourager et reconnaître les initiatives en matière de développement des formations. Il s'agit notamment du label « CyberEdu », destiné aux formations supérieures non spécialisées en cybersécurité, et du label « SecNumEdu » pour les formations de spécialistes en sécurité des systèmes d'information (voir encadré). Plusieurs autres formations actuellement dispensées en région pourraient faire l'objet d'une labellisation Anssi.

Afin de guider les entreprises dans leur politique de recrutement, d'accompagner les porteurs de formation et d'encourager les étudiants ou salariés en reconversion, l'Anssi a produit un « Panorama des métiers de la cybersécurité ». Appellations, missions, compétences, domaines d'intervention, tendances d'évolution sont autant de dimensions qui y sont développées, permettant d'appréhender le marché de l'emploi cyber en pleine essor.

Les métiers en cybersécurité offrent une grande variété. Les experts techniques occupent souvent le devant de la scène, or il y a aussi besoin de managers, de juristes[3], de commerciaux... Au sein d'une même structure, en particulier dans les grands groupes, on peut rencontrer jusqu'à 30 profils différents. Des reconversions sont également possibles. A titre d'exemple, des écoles comme Simplon accueillent des profils non diplômés pour les former aux métiers de la cybersécurité. De plus en plus de postes vont être à pouvoir.

Jean-Pierre Larcher et Philippe Hugo
Mission Stratégie prospective intelligence économique (SPIE)
Région Normandie
spie@normandie.fr

Neuf formations labellisées « Anssi » en Normandie

Huit formations sont labellisées « CyberEdu » de l'Anssi :

- *BTS Services informatiques aux organisations (SIO) du lycée Saint-Adjutor à Vernon*
- *DUT Génie électrique informatique industrielle de l'IUT de l'université Le Havre Normandie*
- *Titre RNCP III Technicien supérieur systèmes et réseaux du centre Afpa de Caen-Ifs*
- *Titre RNCP III Technicien supérieur systèmes et réseaux du centre Afpa de Rouen*
- *Titre RNCP III Développeur web et web mobile du centre Afpa de Caen-Ifs*
- *Titre RNCP III Développeur web et web mobile du centre Afpa de Rouen*
- *Licence professionnelle Systèmes automatisés réseaux et informatique industrielle, parcours Supervision des installations industrielles de l'IUT de l'université Le Havre Normandie*
- *Titre RNCP II Concepteur développeur d'applications du centre Afpa de Rouen*

Et une formation a obtenu le label « SecNumEdu » de l'Anssi :

- *Master informatique, parcours Sécurité des systèmes informatiques (SSI) de l'université de Rouen*

Une veille « Compétences numériques » proposée par le Carif-Oref de Normandie

En lien avec sa stratégie numérique, la Région Normandie a confié au Carif-Oref une mission de veille sur la transformation numérique dans les entreprises et ses effets sur l'évolution de l'emploi, des métiers et des compétences.

Cette veille, mise en œuvre avec l'outil Scoop.it, est accessible à tous. Plus de 80 contenus liés à la cybersécurité y sont référencés (choisir le tag « cybersécurité » pour tous les retrouver).

La veille « Compétences numériques »

S'abonner à la newsletter « Compétences numériques »
(parution toutes les deux semaines, le mardi après-midi)

Documents et outils de référence :

Rapport d'activité 2020 de l'Anssi

« Panorama des métiers de la cybersécurité » de l'Anssi

« Guide des bonnes pratiques de l'informatique » (Anssi / CPME)

« Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures » (Anssi)

Mooc de l'Anssi

Kit de sensibilisation contre la cybermalveillance

[3] Il existe une spécialité juridique cyber au sein du M2 Droit du numérique à l'université de Caen Normandie qui intègre pleinement le sujet « cybersécurité »