CONTEXTE DE LA CYBERSÉCURITÉ

UNE PRIORITÉ MONDIALE…

Depuis une dizaine d'années, les cyberattaques augmentent dans un monde plus connecté (digitalisation des entreprises, généralisation du télétravail, explosion des objets connectés) et créent des tensions internationales. Le Forum Economique Mondial classe les cyberattaques dans les 10 risques majeurs des années à venir.

DÉFINITION

> La cybersécurité recouvre les activités nécessaires pour protéger les réseaux et les systèmes d'information ainsi que les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces.
>
> (Source : Règlement de l'UE sur la cybersécurité)

… QUI CONCERNE TOUTES LES ENTREPRISES

Toutes les structures, quelle que soit leur taille, peuvent être victimes de cyberattaques. Les grands groupes ne sont plus les seules victimes et les attaques se multiplient à l'encontre des PME qui sont devenues une cible prisée des cybercriminels. Certains secteurs sont particulièrement touchés comme la finance, la santé ou encore le commerce en ligne. Selon le ministère de la transition numérique, plus d'une entreprise sur deux, victime d'une cyberattaque, dépose le bilan dans les 18 mois.
Parmi les attaques les plus fréquentes, on peut notamment citer :

Les rançongiciels / ransomware

en 2021, en France, 1 633 entreprises et 312 collectivités ont déclaré des attaques par rançongiciel (*source : rapport de cybermalveillance*).
Ces attaques provoquent des conséquences majeures pour les entreprises.
Les attaquants se font passer pour des prestataires, des fournisseurs ou des clients et demandent à être payés. La France figure notamment dans le Top 3 des pays européens les plus touchés par les rançongiciels selon le baromètre 2022 d'Anozr Way.

Le phishing

les attaquants vont tenter de voler les identifiants de comptes informatiques ce qui va permettre de récupérer de la donnée.
Ils vont chercher à faire cliquer l'utilisateur sur un lien pour installer un virus ou alors une porte dérobée afin d'installer un CryptoMiner, des logiciels permettant de « miner » de la cryptomonnaie.

Menaces d'ingénierie sociale

ces menaces englobent les activités qui tentent d'exploiter une erreur humaine ou un comportement, dans le but d'accéder à des informations ou des services : inciter un utilisateur à ouvrir un document ou visiter un site web, par exemple.

Risques mondiaux perçus par les entreprises

Business

1. Cost-of-living crisis
2. Natural disasters and extreme weather
3. Geoeconomic confrontation
4. Widespread cybercrime and cyber insecurity
5. Largo scale environmental damage incidents
6. Erosion of social cohesion and societal polarization
7. Failure to mitigate climate change
8. Natural resource crises
9. Debt crises
10. Failure of climate-change adaption

Source : Perception survey 2023, World Economic Forum

45 % des entreprises françaises ont subi au moins une cyberattaque en 2022

Le phishing est le vecteur d'attaque le plus courant
Le vol de données et l'usurpation d'identité sont les principales conséquences

6 entreprises sur 10 notent un impact sur leur business notamment une perturbation de leur production

Source : Enquête du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), 2023

ENJEUX

FAIRE DE LA CYBERSÉCURITÉ UN VECTEUR D'INNOVATION

Dans un monde largement numérisé, le chiffrement est une pièce maîtresse de la sécurité. Selon la CNIL, il contribue à faire de la cybersécurité le « vecteur de confiance et d'innovation ».
Les principaux enjeux autour des technologies de cybersécurité sont les suivants :

Protéger les personnes et leur vie privée afin de garantir leurs droits fondamentaux

Protéger les systèmes d'information des entreprises et des États, car les atteintes à ces systèmes peuvent occasionner de graves préjudices économiques et politiques

Promouvoir l'essor de l'économie du numérique, au travers des notions de confiance et de sécurité, pour stimuler l'innovation et la croissance

Maintenir la compétitivité des acteurs nationaux du domaine de la cybersécurité pour soutenir l'économie

QUELS ENJEUX POUR LES ENTREPRISES ?

Placer la gouvernance de la cybersécurité au bon niveau dans l'entreprise

Trouver le bon modèle opérationnel pour la mise en oeuvre des solutions et services de sécurité

Adapter les solutions et les processus à la transformation numérique de l'entreprise

- En premier
- Au total (cite en 1er, en 2e ou en 3e)

Source : Enquête du Club des Experts de la Sécurité de l'Information et du Numérique, 2023

UNE VOLONTÉ POLITIQUE DE RENFORCER LA CYBERSÉCURITÉ

Un cadre réglementaire qui se durcit en Europe

Les députés européens ont voté en novembre 2022 la directive révisée sur la sécurité des réseaux et des systèmes d'information (NIS2). Elle vise à harmoniser et à renforcer la cybersécurité du marché européen. À l'échelle nationale, NIS 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés (parmi eux des entreprises allant des PME aux groupes du CAC40). L'un des changements imposés par NIS2 concerne les obligations de signalement des incidents. NIS2 exige également que les entités concernées mettent en place une liste de mesures de gestion des risques.

Une stratégie d'accélération

Dans le cadre de France 2030, le gouvernement a lancé une stratégie d'accélération « Cybersécurité » destinée à soutenir la filière nationale de cybersécurité et renforcer la souveraineté. À l'horizon 2025, l'objectif assigné à cette stratégie est l'atteinte d'un chiffre d'affaires de 25 Md€ pour la filière (soit un triplement du chiffre d'affaires actuel), le doublement des emplois dans le secteur en passant de 37 000 à 75 000 emplois et l'émergence de trois licornes françaises en cybersécurité. L'inauguration du **Campus Cyber National** en février 2022 est un autre exemple de la volonté française d'organiser de la coopération intersectorielle, publique/privée, autour des grands défis de cybersécurité. C'est typiquement le lieu où pourront être discutés les enjeux de l'arrivée du quantique.

Plusieurs objectifs sont fixés à l'horizon 2025:

x3
Chiffre d'affaires de la filière passant de 7,3 Mds€ à 25 Mds€

x2
Nombre d'emploi dans la filière passant de 37 000 à 75 000

+20%
Nombre de brevets enregistrés par le réseau des SATT at France Brevets

x2
Nombre de thèse CIFRE sur 5 ans passant de 15 à 30 thèses

3
Licornes françaises à faire émerger

+30%
Recherche partenariale

PERSPECTIVES

DES ÉVOLUTIONS À VENIR

Le marché de la cybersécurité va poursuivre sa croissance en France et passerait de 2,8 milliards d'euros en 2021 à 4,2 milliards d'euros en 2025 (+11 % /an) selon la société d'études Markess by Exaegis.

Dans les années à venir, la cybersécurité va recourir de plus en plus à d'autres technologies émergentes : l'intelligence artificielle, la blockchain ou encore le quantique.

Dans le domaine de la blockchain, la technologie permet de ne pas altérer les échanges. La blockchain permet de proposer un service d'authentification.

L'Intelligence Artificielle peut permettre de détecter des comportements malsains ou viraux pouvant avoir lieu sur les systèmes d'informations. Des recherches sont actuellement réalisées dans le domaine. Elles se concentrent notamment sur les EDR (Endpoint Detection and Response), de NDR (Network Detection and Response) ou de XDR (Extended Detection and Response). Il s'agit de l'analyse du comportement d'une machine ou d'un réseau.

Des chercheurs de l'Université de Floride en collaboration avec la CIA espèrent identifier et freiner les menaces cyber en amont grâce à l'intelligence artificielle et les applications d'apprentissage automatique (AIML). Les deux parties mènent conjointement une étude pour tenter de savoir comment ces technologies peuvent être utilisées pour détecter les agents malveillants qui infiltrent les systèmes informatiques.

Le quantique représente par ailleurs un intérêt réel pour la cryptographie. À l'avenir, les ordinateurs quantiques pourront déchiffrer les protocoles de chiffrement utilisés. Il s'agit d'utiliser le quantique pour disposer de systèmes de chiffrement qui seront inviolables par rapport à d'autres ordinateurs quantiques. Les premiers utilisateurs de ces systèmes sont les acteurs qui ont un besoin important de préserver les secrets, notamment tout ce qui est lié à la Défense. Ces technologies du quantique ne sont pas encore matures.

EVALUATION	
Maturité technologique	Impact environnemental
Maturité du marché	Opportunité pour les PME

Légende *Faible* *Moyen* *Fort*

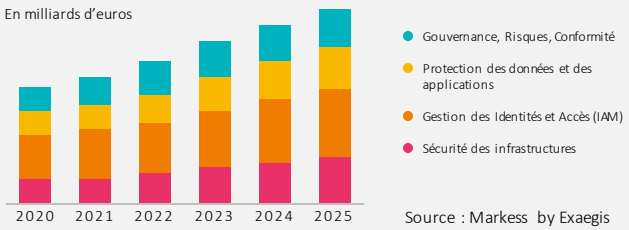
DES IMPACTS ENVIRONNEMENTAUX À ÉVALUER

Si l'impact n'est pas neutre car la cybersécurité nécessite un stockage important d'informations, ces technologies ne semblent pas être plus négatives que des technologies classiques utilisées dans le numérique. Par ailleurs, la cybersécurité permet de réduire des attaques plutôt consommatrices en termes de ressources. Certains attaquants vont voler des accès aux serveurs dans le Cloud. Ces attaquants vont mettre des cryptominers, des petits logiciels qui vont "miner du bitcoin". Cela va représenter des consommations importantes de serveurs et d'énergie.

Un groupe de travail cyber-énergie a été monté au sein du Clusif. Avec pour objectif, sensibiliser sur les impacts de coupure électrique, sur le système d'information, mais aussi l'impact que cela peut avoir d'un point de vue cyber. Mais n'oublions pas que la cybersécurité induit une maîtrise de tout ce qui se connecte.

Benoît Fuzeau, Président de l'Association Le CLUSIF

Prévisions de croissance du marché de la cybersécurité en France



Source : Markess by Exaegis

La cryptographie quantique et post-quantique sont aussi des solutions à étudier pour mieux nous protéger.

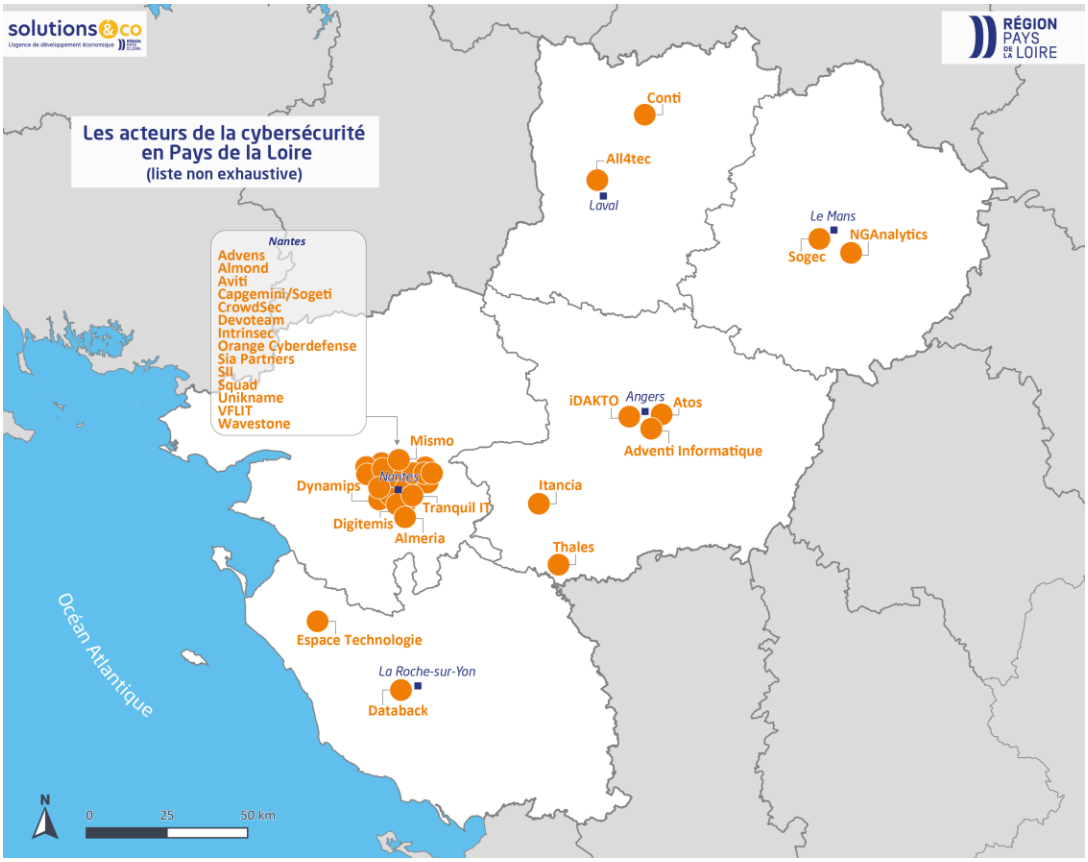
Benoît Fuzeau, Président de l'Association Le CLUSIF

Le chiffrement quantique reste du domaine de l'innovation technologique. C'est très émergent et très spécialisé. La plupart des sociétés faisant du Quantum Computing sont des sociétés soit dans la recherche, soit en phase de capitalisation.

Jean-Noël De Galzain, Directeur Général de Wallix

LA CYBERSECURITE EN PAYS DE LA LOIRE

CARTOGRAPHIE DES ENTREPRISES



Source : Analyse DAP – ANSSI

Les Pays de la Loire sont caractérisés par un écosystème de prestataires de services et de conseils de la cybersécurité. On constate une opportunité de développement autour de l'accompagnement des TPE & PME, notamment pour les réponses aux incidents.
Les éditeurs de solutions de cybersécurité restent cependant assez restreints en région.

> *En Pays de la Loire, il y a différents niveaux d'expertise. Il y a d'un côté des prestataires qualifiés par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour répondre aux besoins les plus hauts en matière de sécurisation. De l'autre, une vingtaine de prestataires labellisés par cybermalveillance.gouv.fr pour répondre aux besoins de sécurisation standards. Pour les Pays de la Loire, il faudrait multiplier ce chiffre par 3 ou 4.*
>
> Régis DUBRULLE – ANSSI

LA CYBERSECURITE EN PAYS DE LA LOIRE

DE NOMBREUX PROJETS DE RECRUTEMENTS

Au cœur des préoccupations régionales, la cybersécurité est une filière d'avenir qui crée de nouvelles opportunités d'emplois. Parmi les projets en cours de développement, citons par exemple le projet **d'usine du futur d'Atos à Angers**, dédié à la production de supercalculateurs, serveurs hauts-de-gamme et produits de cryptologie et cybersécurité.
À terme, ce projet va permettre la création d'une centaine d'emplois qualifiés et va faire de l'usine un véritable centre d'innovation européen.
À Nantes, **la Maison de l'innovation du Groupe La Poste** est en construction et accueillera entre 800 et 1 000 informaticiens entièrement voués à l'activité cybersécurité du Groupe.
Le site choletais du groupe de défense Thales est en plein essor sur les systèmes de télécommunication sécurisés et la cybersécurité. Thales a l'ambition de passer de 1 800 à près de 2 500 salariés d'ici trois ans sur ce site.
Magellan Sécurité qui propose des prestations de conseil et d'intégration de solutions de sécurité, annonce également des perspectives de recrutement en 2023 pour son agence de Nantes.
Enfin, des acteurs majeurs de la cybersécurité en région tels que **Digitemis, Advens** et **Almond** devraient étoffer leurs équipes d'ici fin 2023.

La Poste ouvrira une maison de l'innovation à Nantes en 2024

DES FORMATIONS SUR L'ENSEMBLE DU TERRITOIRE

63 formations dans la cybersécurité

Source : CARIF-OREF, ONISEP, CPF, GEN

Les formations en cybersécurité sont maillées sur l'ensemble des départements des Pays de la Loire, délivrant des diplômes allant du technicien à l'ingénieur.
Plusieurs formations sont labellisées **SecNumedu** par **l'ANSSI.** C'est notamment le cas du diplôme d'ingénieur **de l'ESIEA** option cybersécurité du campus de Laval (53). L'ESIEA dispose **d'un laboratoire CNS (Confiance Numérique et Sécurité)** abordant l'ensemble des domaines liés à la cybersécurité et son éthique. Il vise à garantir pour les particuliers et les entreprises, l'intégrité des transactions, la confiance et la protection du patrimoine informationnel.
L'ANSSI a labellisé plusieurs autres formations telles que la licence professionnelle des métiers de l'informatique – Administration et sécurité des systèmes et des réseaux de **l'IUT de la Roche-sur-Yon** (85), le Master spécialisé en cybersécurité de l'**IMT Atlantique Pays de la Loire** (44) et la formation ingénieur du numérique majeure cybersécurité et réseaux de **l'ESAIP** (49). D'autres formations (initiales ou adultes, non labellisées) sont assurées sur la cybersécurité notamment au sein de **la Fab'Academy** (44) ou le **CESI** (72).
Enfin, **Airbus** et **Ynov campus**, école formant aux métiers du digital et des nouvelles technologies, s'associent pour lancer en septembre 2023 un Master spécialement conçu pour former les futurs professionnels de la cybersécurité de l'industrie aéronautique, spatiale et de la défense.

La cybersécurité est un secteur stratégique qui va énormément se développer dans les années à venir. C'est une opportunité pour les territoires. (…) La cybersécurité est créatrice d'emplois dans tous les domaines, dans tous les secteurs.
Jean-Noël De Galzain, WALLIX

En Pays de la Loire, il y a un développement de formations en lien avec la Cybersécurité : IUMM (enseignement supérieur), Ecoles d'Ingénieur. Ces formations sont en développement dans la Région depuis trois ans.
Régis DUBRULLE – ANSSI

Le futur campus Cyber, qui devrait s'implanter en région, devrait permettre un développement de la cybersécurité.
Frédéric DANIEL – ORANGE CYBERDEFENSE

POTENTIEL POUR LES PME

BÉNÉFICES ATTENDUS

Sensibiliser les salariés, anticiper les failles et connaître les réactions en cas d'attaque

Se développer sur un marché en croissance pour les sociétés spécialisées

Combiner l'expertise de filières industrielles avec la cybersécurité

> La cybersécurité a un réel intérêt. Une société victime d'un ransomware va enregistrer des pertes financières. Cela peut représenter plusieurs jours d'arrêt et d'importantes pertes financières. La cybersécurité ne nécessite pas un gros investissement initial. Ce sont des petites actions à mettre en œuvre.
> **Alexandre AMBIEHL - E-COBOT**

> Pour les PME en Pays de la Loire, il y a des opportunités en matière de créations de solutions de détection et d'authentification. Il faut aller vers la protection des environnements biomédicaux, industriels, l'IOT. Il y a un savoir-faire autour ces sujets.
> **Frédéric DANIEL – ORANGE CYBERDEFENSE**

> Une analyse de risque détermine les mesures devant être mise en œuvre pour réduire les risques du projet. Ces mesures sont ensuite chiffrées et détermineront la prise de décision, afin de trouver le meilleur équilibre "coûts/risques". Les budgets cybersécurité se situent en général autour de 5 à 10 % du budget DSI.
> **Benoît Fuzeau, CLUSIF**