Région Bretagne

idéo
Le service public de l'orientation

FOCUS

LA CYBERSÉCURITÉ EN BRETAGNE

© Adobe stock

© Adobe stock

Avec près de 8 000 postes, la Bretagne est la 2e région cyber de France.

La multiplication des usages et des équipements numériques ont conduit à **une hausse importante des cyberattaques**. En conséquence, les besoins en personnels qualifiés en sécurité informatique explosent.

Emploi, recherche, formation, la Bretagne constitue **une des principales régions cyber en France**. Des institutions importantes y sont installées, notamment dans la métropole rennaise (Direction générale de l'armement, Commandement de la cyberdéfense, Agence nationale de la sécurité des systèmes d'information, etc.) mais aussi de grands groupes (Orange, Airbus, Thalès, etc.) et des start-up.

Sommaire

“Nous utilisons l’intelligence artificielle pour faire évoluer nos outils face à la masse de données que nous avons à traiter”

Colonel Pierre-Arnaud Borrelly, ex-commandant du groupement de cyberdéfense des armées

© Marcus Spiske / Unsplash

LES CHIFFRES CLÉS

Les attaques sur les systèmes informatiques se multiplient en France et avec elles les besoins en sécurité de l'État, des entreprises, des administrations, etc. Résultat, en 2025, le marché de la cybersécurité en France devrait atteindre **3,5 milliards d'euros, soit une hausse de 18 % par rapport à 2024**.

La Bretagne est désormais la **2e région cyber en France** en termes d'emplois derrière l'Ile-de-France. Elle se compose d'un **écosystème hétérogène d'acteurs** : start-up, grands groupes (Thalès, Orange, Airbus, etc.), institutions (Anssi, Commandement de la cyberdéfense, Direction générale de l'armement), pépinières d'entreprises (Digital square, etc.), établissements d'enseignement supérieur et de recherche, etc.

Si une bonne partie des emplois se concentrent dans la **métropole rennaise**, on trouve aussi des structures dédiées à la cybersécurité à **Lannion, Brest, Vannes et Lorient**.

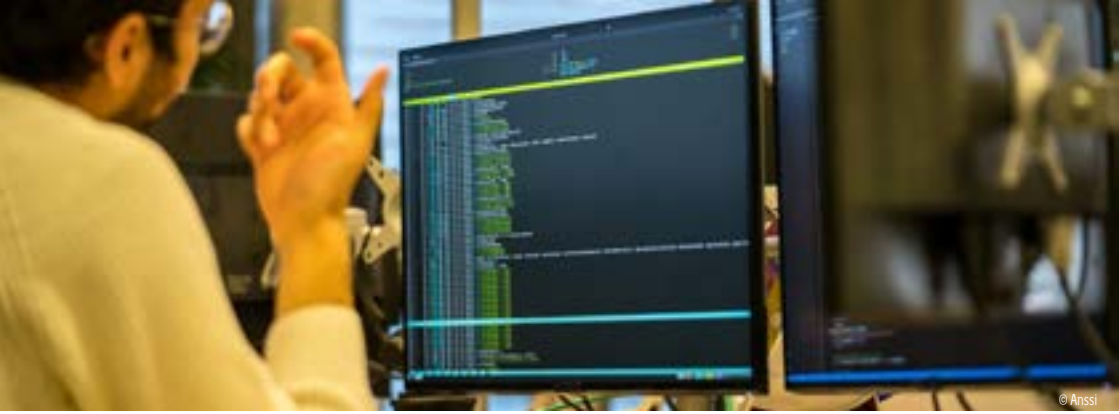
La Bretagne est désormais la 2e région cyber en France en termes d'emplois.

170
entreprises

45
équipes de recherche

70
formations

8 000
emplois


© Anssi

VOS QUESTIONS

Doit-on forcément être militaire ?

Non, **il n'est pas obligatoire d'être militaire pour travailler dans la cybersécurité**, loin de là. En Bretagne, on compte **8 000 emplois** dans le secteur, qui sont **majoritairement occupés par des civils**.

Au sein même de l'armée, un quart des personnels en cyber sont des civils. Le secteur est composé d'une grande variété de structures : grands groupes, start-up, PME, etc.

Doit-on faire de longues études ?

Dans une enquête menée en 2021, l'Anssi (Agence nationale de la sécurité des systèmes d'information) constate que « *plus des trois quarts des professionnels possèdent un diplôme ou un niveau de qualification supérieur ou égal à bac+5* ».

Même constat au Groupement de cyberdéfense des armées même si la situation évolue peu à peu : « *nous avons **beaucoup d'ingénieur·es mais nous recrutons de plus en plus de bac +2 ou +3** avec l'ambition de les former en interne* » affirme le colonel Pierre-Arnaud Borrelly, ex-commandant du Groupement de cyberdéfense des armées.

Pour Vivien Bernet-Rollande, directeur technique de CT- Square, qui fournit des services cyber aux PME et ETI, « *il n'y a pas assez d'ingénieurs sur le marché de l'emploi. Le meilleur moyen de résoudre ce problème est d'avoir des ingénieurs seulement pour fournir des outils et des procédures qui vont permettre à d'autres gens de les mettre en place* ».

Y a-t-il beaucoup de femmes dans la cybersécurité ?

Selon l'Anssi, **les femmes sont très minoritaires** dans la cybersécurité où elles représentent à peine 12% des effectifs.

Le **programme « Cadette de la cyber** » mené par le Pôle d'excellence cyber, **vise à encourager les femmes à rejoindre ce secteur**.

Est-ce un secteur qui recrute beaucoup ?

Les embauches augmentent d'année en année mais le secteur peine à trouver suffisamment de candidat·es. Au niveau des pouvoirs publics, les recrutements sont au vert : l'armée souhaite passer de 800 personnes en 2019 à 1 800 personnes en 2025, le budget prévu par la loi de programmation militaire est en forte hausse, l'Anssi a installé une antenne à Rennes, etc.

Le secteur privé n'est pas en reste avec la p**résence de grands groupes** (Orange, Airbus, Thalès, etc.), de start-up et de **pépinières spécialisées**. Au total, cela représente 160 entreprises pour la région.

Retrouvez l'intégralité des réponses sur ***ideo.bretagne.bzh***

ET DEMAIN ?

IA, objets connectés, clouds : les nouvelles technologies bouleversent la cyber

L'intelligence artificielle (IA) va augmenter le nombre et la sophistication des menaces potentielles. « *Cela va permettre l'automatisation d'un certain nombre de tâches pour mener des attaques* », explique Laurent Dubau, manager chez Orange Cyberdefense. Des mécanismes permettent ainsi d'usurper des identités, notamment en imitant une voix ou un visage.

Mais l'IA peut également être un allié efficace : « *Nous utilisons l'intelligence artificielle pour faire évoluer nos outils* », explique le Colonel Pierre-Arnaud Borrelly. Plus généralement, les nouveaux outils grands publics tels que Chat GPT ou le métavers représentent de nouveaux enjeux.

Les objets connectés sont de plus en plus courants dans notre quotidien. Selon le cabinet de tendances WGSN, il pourrait y en avoir 50 milliards sur le marché en 2030. « *La sécurité aujourd'hui dans le domaine des objets connectés est du niveau de ce qu'on avait sur les autres systèmes dans les années 90'. Le fait de connecter tout et n'importe quoi sur internet peut présenter des risques importants* », explique Vivien Bernet-Rollande, directeur technique de CT-Square.

« *Ces objets sont parfois fabriqués dans des pays tiers qui n'ont pas forcément les mêmes exigences en termes de cybersécurité que nous. S'ils sont mal sécurisés, ils se révèlent très intéressants pour les pirates car ils peuvent être pris en contrôle à distance* », explique Laurent Dubau.

Les services à distance appelés software as a service (SaaS), sous-catégorie du cloud, se sont eux-aussi multipliés ces dernières années. « *Les entreprises externalisent de plus en plus d'informations via le transfert de fichiers, par exemple sur des plateformes numériques. Ça génère beaucoup de nouvelles menaces* », selon Laurent Dubau.

Vivien Bernet-Rollande renchérit : « *Quand les données sont hébergées chez quelqu'un d'autre, c'est difficile de mettre* en place des capacités de détection. »

Règlementations : après le RGPD, voici NIS 2

Les exigences réglementaires ont augmenté en quelques années, notamment avec le RGPD (Règlement général sur la protection des données). La prochaine étape sera la traduction d'une directive européenne appelée NIS 2 (Network Information Security).

« Elle demande à un certain nombre d'acteurs de se sécuriser. Ça aura un impact sur les organisations car le suivi de la conformité, l'identification des systèmes essentiels et les mesures de protection nécessiteront des ressources supplémentaires », affirme Laurent Dubau.

Limiter les opérations d'influence

Campagnes de dénigrement, diffusions massives de fake news, tentatives de déstabilisation : ces sujets sont devenus des préoccupations récurrentes dans de nombreux pays. *« Ces opérations ne demandent pas de réaliser des intrusions : il s'agit simplement de produire du contenu sur des réseaux sociaux, d'écrire des commentaires sous des articles de journaux, etc. Les réponses à ce phénomène vont peut-être se développer dans les prochaines années »*, *analyse Vivien Bernet-Rollande.*

Si ces problématiques sont souvent évoquées d'un point de vue géopolitique, elles peuvent aussi toucher des petites structures. *« Vous avez des entreprises qui postent des faux avis google sur la page de vos concurrents en échange d'argent. Cela dégrade la qualité de l'information »*, complète-t-il.

> ***«l'IA va permettre l'automatisation d'un certain nombre de tâches pour mener des attaques.»***
>
> **Laurent Dubau,**
> *manager chez Orange cyberdéfense*

© Emiliano Vittoriosi / Unsplash

LES MÉTIERS

Quelques exemples de métiers dans la cybersécurité

Gestion de la sécurité & pilotage des projets de sécurité


© Gabrielle Cezard / Anssi

Responsable de la Sécurité des Systèmes d'Information (RSSI)

Il assure le pilotage de la démarche de cybersécurité. Il définit ou décline la politique de sécurité des systèmes d'information (prévention, protection, détection, etc.) et veille à son application. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeur·trices métiers.

Conception et maintien d'un système d'information sécurisé


© Jérôme Sevrette

Architecte sécurité

Il assure que les choix techniques et technologiques des projets et métiers respectent les exigences de sécurité de l'organisation. Il définit les modèles de sécurité et accompagne le développement des architectures de sécurité au sein du système d'information en cohérence avec la stratégie IT (pour technologie de l'information) et les politiques de sécurité de l'organisation.

Hacker éthique

Les hackers éthiques sont des pirates informatiques bienveillants qui testent et identifient les failles des systèmes et des réseaux informatiques des entreprises pour prévenir et neutraliser de potentielles attaques internes ou externes.

Cryptologue

Expert en sécurité des systèmes de communication, le cryptologue chiffre et déchiffre des informations numériques sensibles. Mathématicien de formation, il travaille à partir d'algorithmes complexes qu'il doit sans cesse améliorer.

Gestion des incidents et des crises de sécurit

Opérateur / Opératrice analyste SOC (Security Operater Center)

Il assure la supervision du système d'information de l'organisation afin de détecter des activités suspectes ou malveillantes. Il identifie, catégorise, analyse et qualifie les incidents à partir de rapports d'analyse sur les menaces. Il contribue au traitement des incidents de sécurité.

Pour plus d'informations sur les métiers

Conseil, services et recherche


© Jérôme Sevrette

Consultant / Consultante en cybersécurité

Il propose, à partir d'un diagnostic, des solutions, méthodes, outils et autres qui répondent aux enjeux posés. Il mobilise pour ce faire des éléments issus de son expertise et de son expérience ainsi que des outils développés en interne. Il anticipe les évolutions du contexte de cybersécurité, apporte un retour d'expérience et une vision des pratiques du marché. Il apporte son expertise aussi bien sur des sujets méthodologiques que techniques.

Métiers connexes

© Jérôme Sevrette


Jérôme Sevrette

Délégué / Déléguée à la protection des données (DPD)

Il est chargé de mettre en œuvre la conformité au Règlement européen sur la protection des données (RGPD) au sein de l'organisation qui l'a désigné. Il s'intéresse également au risque lié à l'utilisation de la donnée sur la vie privée des personnes concernées.


© Franck Betermin

Juriste spécialisée en cybersécurité

Il peut éclairer une organisation sur les conséquences pénales ou civiles d'une cyberattaque. Il est un acteur essentiel de la contractualisation avec les fournisseurs en intégrant des clauses de sécurité en collaboration étroite avec les équipes cybersécurité

LES FORMATIONS

Quelques exemples de formations dans les énergies renouvelables

Après le BAC

BAC +2

- BTS Cybersécurité, informatique et réseaux, électronique option A informatique et réseaux
- BTS Cybersécurité, informatique et réseaux, électronique option B électronique et réseaux

BAC +3

- BUT Réseaux & télécommunications parcours cybersécurité
- Licence pro Métiers des réseaux informatiques et télécommunications

BAC +5

- Diplôme d'ingénieur de l'École nationale supérieure de sciences appliquées et de technologie de Lannion (Enssat)
- Master Ingénierie des systèmes complexes
- Master Mathématiques et applications parcours mathématiques de l'information cryptographie

Des formations labellisées par l'Anssi

L'Anssi (Agence nationale de la sécurité des systèmes d'information) a mis en place le label SecNumedu. Il permet de s'assurer que la formation dans le domaine de la sécurité du numérique répond à une charte et des critères définis.

Quelques exemples de formation continue

- Mastère spécialisé cybersécurité
- Diplôme d'ingénieur cyberdéfense de l'École nationale supérieure d'ingénieurs de Bretagne Sud (Ensibs)

Pour plus d'informations sur les formations

SOURCES ET RESSOURCES

Des ressources pour aller plus loin

- Panorama des métiers de la cyber
- Le site gouvernemental de prévention en sécurité numérique
- Le MOOC de l'Agence nationale de la sécurité des systèmes d'information (Anssi)
- Page officielle du Commandement de cyberdéfense
- Semaine européenne de la cybersécurité de Rennes
- Une collection de témoignages de professionnel·les de la cyber

Sources utilisées dans ce Focus

- APEC (en partenariat avec le Pôle d'excellence cyber), Cybersécurité, un marché de l'emploi cadre diversifié et de plus en plus porteur, 2022
- Anssi, Panorama des métiers de la cyber, 2020
- Métiers du numérique en Bretagne : une activité en pleine croissance, Gref Bretagne, 2024

Pour plus d'informations sur les métiers

RDV sur ideo.bretagne.bzh/metiers

© Taylor Vick / Unsplash

Nos derniers Focus

Aide et accompagnement à domicile
Agriculture et paysage
Agroalimentaire
Bâtiment
Forêt et bois
Énergies renouvelables
Festival
Numérique
Métallurgie
Métiers de bouche
Métiers de la Défense
Nautisme
Pêche & aquaculture
Sport
Tourisme
Travaux publics

Plus d'informations sur

ideo.bretagne.bzh

Le service public de l'orientation

283 avenue du Général Patton – CS 21101 – 35 711 Rennes cedex 7
Tél. : 02 99 27 10 10 | @regionbretagne.bsky.social | facebook.com/regionbretagne.bzh | region.bretagne
www.bretagne.bzh

Novembre 2025 – Conception : R2/Région Bretagne