LA FRANCE INVESTIT POUR LA CYBERSÉCURITÉ

LÉA NOÉ

NOVEMBRE 2021

DEF'INSEEC DEFINSEEC@GMAIL.COM 0 6 6 6 7 3 7 1 6 5

LA FRANCE SEMBLE AVOIR SAISIE L'IMPORTANCE DE LA CYBERSÉCURITÉ

Depuis quelques années maintenant, la France s'intéresse et se positionne sur les enjeux de cybersécurité. Cet intérêt a pu naître à la suite de rapports parlementaires et sénatoriaux, comme celui de Pierre Lasbordes en 2006, celui de Roger Romani en 2007 ou même celui de Jean-Marie Bockel en 2012. Ces trois rapports français ont permis la mise en lumière des thématiques de cyberdéfense. L'intérêt de la France s'est aussi affirmé via la création de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) en 2009, via la mise en place de la Stratégie nationale pour la sécurité du numérique (2015) ou même via la Stratégie internationale de la France pour le numérique (2017). La France a su appuyer ses ambitions par des dispositifs et ainsi tenter de faire face aux menaces croissantes du cyber.

Crédit photo : Canva

Crédit photo : Les Échos

On retrouve cette évolution et cette mise à l'agenda des problématiques de cybersécurité au sein des différents Livres Blancs. Le Livre Blanc de 2008 mentionnait le cyberespace et le qualifiait de "nouveau champ d'action dans lequel se déroulent déjà des opérations militaires", celui de 2013 mettait en lumière la volonté de protection des infrastructures critiques et le développement de capacités offensives. Enfin, le Livre Blanc de 2018, fixait les grandes lignes du modèle français et présentait le principe de séparation du défensif et de l'offensif ainsi que le concept de souveraineté numérique.

Les multiples confinements ainsi que la démocratisation du télétravail ont mis en lumière, de façon plus accrue, l'importance d'une cybersécurité à l'échelle locale mais surtout à l'échelle nationale. Le nombre de cyberattaques a connu une croissance relativement régulière jusqu'en 2019. En 2020, le nombre d'attaques par rançongiciels[1] traitées par l'ANSSI a été multiplié par 4 par rapport à l'année précédente. Les hôpitaux font aujourd'hui face à des attaques informatiques de façon hebdomadaire[2]. Les attaques par rançongiciels sont d'ailleurs aujourd'hui considérées comme la première menace pour les entreprises et les collectivités en 2020.

[1] Rançongiciel ou ransomware : logiciel malveillant qui peut bloquer l'accès à un ordinateur, un téléphone portable ou bien chiffrer des données personnelles.

[2] Cédric O, interrogé au Sénat lors des questions au gouvernement sur l'attaque ayant ciblé le centre hospitalier de Dax (Landes) dans la nuit du 8 au 9 février.

LA FRANCE INVESTIT POUR LA CYBERSÉCURITÉ

1 milliard d'euros

LE PLAN À 1 MILLIARD D'EUROS

En réaction à ces cyberattaques et au manque de protection et de préparation des entreprises et collectivités, le gouvernement français a lancé, début 2021, un plan à 1 milliard d'euros pour renforcer la cybersécurité d'ici 2025.

Ce plan contient six objectifs clés :

1. Multiplier par 3 le chiffre d'affaires de la filière (de 7,3 milliards à 25 milliards d'euro)
2. Obtenir un meilleur positionnement de la France par rapport aux concurrents internationaux en doublant les emplois dans la filière (en passant de 37 000 emplois à 75 000)
3. Augmenter le nombre d'entreprises françaises dans le domaine
4. Faire émerger 3 têtes françaises en cyber
5. Diffuser une véritable culture de la cybersécurité dans les entreprises
6. Stimuler la recherche française en cyber et l'innovation industrielle

En somme, ce plan vise à développer des solutions souveraines, à renforcer les actions et la coopération entre les acteurs du secteur ainsi qu'à soutenir et former les professionnels aux métiers de la cybersécurité.

LES FINANCEMENTS DE CE PLAN

Pour combler les lacunes de la France et booster le business de la cybersécurité en France, le gouvernement a décidé de mobiliser 1 milliard d'euros, et ce, par l'intermédiaire de France Relance et du Programme d'investissement d'avenir. Ces financements sont alors majoritairement composés de fonds publics à hauteur de 720 millions et d'une minorité de fonds privés.

LES DESTINATAIRES ET OBJECTIFS DE CES FINANCEMENTS

En vue de rattraper les leaders du marché de la cybersécurité, il a été décidé qu'un peu plus de la moitié du budget final concernera les travaux de recherche et de développement. De façon décroissante, le budget sera alloué à un plan d'investissement dédié aux start-ups, à la création d'un Cyber Campus à la Défense (20 000m2) pour regrouper les différents acteurs du domaine, au renforcement des moyens de l'ANSSI et pour finir à la formation de « pompiers locaux » qui pourraient intervenir localement en cas d'attaques.

ET AILLEURS ?

La France n’est pas la seule à mettre de nombreux moyens dans ce domaine. Successivement, les États-Unis et la Chine ont eux aussi présenté, cette année, leurs plans en matière de cybersécurité.

Crédit photo : CNew york

LES ÉTATS-UNIS : UN DÉCRET

Après de nombreuses cyberattaques cette année, le président américain a signé, en mai dernier, un décret visant à renforcer la cybersécurité via la modernisation des défenses du pays et via une meilleure coopération entre les victimes et les forces de l’ordre

Crédit photo : Courrier Arabe

LA CHINE : UN PLAN SUR TROIS ANS

L’été dernier, la Chine a elle aussi annoncé la mise en place d’un plan sur trois ans pour protéger ses données à l’intérieur et à l’extérieur de ses frontières et pour stimuler le secteur de la cybersécurité dans le pays. Il est clair que l’objectif premier de ce plan est d’exploiter le fort potentiel du secteur et de générer de nouveaux revenus.

Pour conclure, il est possible de voir, à travers ce plan, les objectifs ambitieux du gouvernement français en matière de cybersécurité. Le Cyber Campus pourrait changer la donne dans le domaine et pourrait pousser la France sur le devant de la scène internationale, répondant ainsi à l'objectif de ce plan.

SOURCES

Anonyme (2021). Chiffres et tendances des cybermenaces : Cybermalveillance.gouv.fr dévoile son rapport d'activité 2020. Consulté le 22/11/2021. [En ligne]. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2020

Anonyme (2021). Cybersécurité, faire face à la menace : la stratégie française. Consulté le 22/11/2021. [En ligne]. https://www.ssi.gouv.fr/actualite/cybersecurite-faire-face-a-la-menace-la-strategie-francaise/

Anonyme (2021). Un campus dédié à la cybersécurité. Consulté le 22/11/2021. [En ligne]. https://www.ssi.gouv.fr/agence/cybersecurite/un-campus-dedie-a-la-cybersecurite/

Anonyme (2021). Un plan à 1 milliard d'euros pour renforcer la cybersécurité. Consulté le 22/11/2021. [En ligne]. https://www.bercynumerique.finances.gouv.fr/index.php/l-information-en-continu/un-plan-a-1-milliard-deuros-pour-renforcer-la-cybersecurite

Anonyme (2021). Un plan à 1 milliard d'euros pour renforcer la cybersécurité. Consulté le 22/11/2021. [En ligne]. https://www.gouvernement.fr/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite

Biden, J. (2021). Executive Order on Improving the Nation's Cybersecurity. Consulté le 22/11/2021. [En ligne]. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Cornwell, S. et Brice, M. (2021). USA-Le Congrès adopte le plan de $1.000 mds de Biden sur les infrastructures. Consulté le 22/11/2021. [En ligne]. https://www.zonebourse.com/actualite-bourse/USA-Le-Congres-adopte-le-plan-de-1-000-mds-de-Biden-sur-les-infrastructures--36927419/?countview=0

Terrasson, B. (2021). La Chine prépare un plan sur trois ans pour stimuler son secteur de la cybersécurité. Consulté le 22/11/2021. [En ligne]. https://siecledigital.fr/2021/07/15/chine-plan-cybersecurite/

Verge, P. (2021). Cybersécurité : le gouvernement américain veut corriger des centaines de failles informatiques. Consulté le 22/11/2021. [En ligne]. https://www.lesechos.fr/tech-medias/hightech/cybersecurite-le-gouvernement-americain-veut-corriger-des-centaines-de-failles-informatiques-1360968

H.E.I.P
AEROSPACE
CYBERSECURITY
DEF'INSEEC

SUIVEZ DEF'INSEEC SUR

DEF'INSEEC DEFINSEEC@GMAIL.COM 06 66 73 71 65