L'AGEFI Quotidien EDITION DE 7 H

PAYS : France
PAGE(S) :25;26
SURFACE :130 %
PERIODICITE : Quotidien

RUBRIQUE : Autre
DIFFUSION :(13000)
JOURNALISTE : Alexandra Oubrier

► **30 octobre 2023**

Cybersécurité, un enjeu de souveraineté pour la France

Jean-Noël Barrot, ministre délégué chargé du numérique, lors de l'université d'été Hexatrust, le 19 septembre 2023 à Paris. ©Hexatrust

La cybersécurité est devenue un sujet stratégique pour l'Hexagone et pour l'Europe, ce qui passe par une règlementation plus exigeante et par des moyens supplémentaires afin d'élever le niveau de protection de tous.

L'Anssi a beaucoup de travail. Cette Agence nationale de sécurité des systèmes d'information, fondée en 2008, est devenue le chef de file de la cybersécurité en France. Mais elle concentre son action directe sur les services de l'Etat et sur les grandes entreprises. Or, la numérisation de l'économie accélérée depuis la crise sanitaire a considérablement augmenté la vulnérabilité des petites et moyennes entreprises et, notamment, des commerçants qui se sont tournés vers la vente sur internet.

Les cyberattaques se sont multipliées et changent de nature. L'extorsion de fonds par le chantage au ransomware ou à la divulgation de données s'est largement répandue. Le phénomène est désormais presque industriel, quasiment toutes les entreprises sont touchées. Et l'expérience montre qu'une PME sur deux ayant subi une telle attaque fait faillite dans les dix-huit mois.

La cybersécurité est donc une question de survie du tissu économique. Et un enjeu de souveraineté technologique, car trop souvent, les entreprises se tournent vers des prestataires de services américains ou non européens.

C'est pourquoi Jean-Noël Barrot, ministre délégué chargé de la transition numérique, a annoncé en septembre 2022 un plan de 30 millions d'euros dont une partie devait servir au développement d'un outil d'autodiagnostic gratuit pour toutes les entreprises et à la mise en place d'un «bouclier cyber» intégrant un audit, ainsi que des formations et solutions pour 750 PME et ETI. La bonne volonté est là, mais ça ne suffira pas.

A lire aussi: Bpifrance au cyber-chevet des PME

Toute une filière mobilisée

C'est toute la filière technologique cyber qui se mobilise désormais, notamment l'association Hexatrust qui regroupe près d'une centaine d'acteurs français et européens de la cyber et du cloud, de confiance, offrant un large catalogue de solutions de cybersécurité. Présidée par Jean-Noël de Galzain, également fondateur et dirigeant de la société Wallix, Hexatrust a publié l'année dernière un Manifeste pour la souveraineté, pour une nouvelle ambition numérique. Il s'agit clairement de soutenir les entreprises françaises et européennes par le biais de la commande publique. Celle-ci est vue comme « *un élément stratégique du développement de ces technologies. La création d'un cadre favorable à la confiance et à la sécurité participera à l'émergence des prochaines générations d'offres technologiques européennes.* »

L'élévation du niveau général de cybersécurité passe par un rapprochement entre secteurs public et privé. La prise de conscience se concrétise : lors de l'université d'été 2023 d'Hexatrust, la signature de deux contrats de filière a été annoncée. Mais les entreprises peuvent aussi agir par elles-mêmes. Un baromètre de la souveraineté numérique a été dévoilé montrant que trois banques étaient classées parmi les entreprises les plus consommatrices de solutions françaises : le Crédit Agricole (1), BNP Paribas (5) et la Société Générale (16). Et l'initiative «Je choisis la French Tech» lancée par le gouvernement en juin dernier contribue à mettre en lumière les technologies hexagonales, y compris dans le domaine cyber.

A lire aussi: Le projet européen Dora explore le risque cyber des banques

L'AGEFI Quotidien EDITION DE 7 H

PAYS : France
PAGE(S) :25;26
SURFACE :130 %
PERIODICITE : Quotidien

RUBRIQUE : Autre
DIFFUSION :(13000)
JOURNALISTE : Alexandra Oubrier

► **30 octobre 2023**

Toutes les entreprises sont concernées

En parallèle, la réglementation évolue et touche désormais presque toutes les entreprises, avec DORA, la directive sur la résilience opérationnelle et NIS2, celle qui prévoit de nouvelles obligations de cybersécurité pour les entités publiques ou privées.

Pour Vincent Strubel, directeur de l'Anssi qui intervenait à l'Université d'été Hexatrust, «*l'enjeu est le passage à l'échelle de la cybersécurité grâce à une panoplie de solutions adaptées aux petites entreprises.* La directive NIS 2 (Network and Information Security) *amène un changement de paradigme : le nombre d'acteurs régulés va être multiplié par dix ou plus, il va falloir travailler différemment, dans une logique d'objectif plutôt que prescriptive. Et dans le domaine du cloud, l'Anssi reste sur la même position : la sécurité doit s'appuyer sur la technologie, sur l'organisation et sur le droit.*» Cela se matérialise par le référentiel SecNumCloud qui est un peu le socle de la politique de souveraineté numérique en France, et qui nécessite encore beaucoup de pédagogie.

A lire aussi: Engie confie sa cybersécurité à Thales

Immunité au droit extra-territorial

Réputé très exigeant, ce référentiel comporte des obligations très fortes, en particulier sur l'immunité aux règles extraterritoriales, comme le Cloud Act et le Fisa américains, en particulier, qui peuvent contraindre des acteurs américains à transmettre des données à leur gouvernement, où qu'elles soient hébergées. Les grands fournisseurs de cloud américains qui dominent le marché sont donc dans la ligne de mire.

La difficulté concernant SecNumCloud est de susciter une adoption large au niveau européen et d'éviter que ce référentiel reste une norme franco-française de souveraineté numérique. Jean-Noël Barrot a bien expliqué la délicatesse de la négociation européenne sur le sujet, évoquant les « *puissants vents contraires* » auxquels se heurte l'initiative française, accusée de vouloir imposer ses propres solutions. «*L'objectif est d'avoir un SecNumCloud européen*, a-t-il assuré, *mais il ne faut pas aller trop vite pour ne pas donner d'arguments à nos adversaires.*»

Pour favoriser l'adoption de SecNumCloud en France et contribuer à déployer les normes élevées de cybersécurité, Bpifrance a été chargée par l'Anssi et la direction des entreprises de Bercy de proposer un accompagnement aux PME souhaitant se faire qualifier SecNumCloud. Une enveloppe de 3,5 millions d'euros a été mobilisée dans le cadre de la stratégie cloud de France 2030. Résultat : 150 entreprises ont déposé une candidature, le ticket maximal par dossier était de 180.000 euros par module financé, parmi quatre modules possibles (audit par rapport à SecNumCloud, préparation de la démarche de qualification, mise en conformité, aide à la qualification). Le nombre est encore modeste, mais le niveau d'exigence de SecNumCloud n'est pas à la portée de toutes les entreprises. La montée du niveau de cybersécurité prendra encore du temps, mais au moins, elle est lancée.

Alexandra Oubrier