



Lettre info

Alliance pour la Confiance Numérique

Mars 2018

Edito

ACN : allier le savoir-faire et le faire-savoir

La confiance numérique est toujours plus au cœur de l'ensemble des sujets sociétaux. La numérisation de toutes les activités pose sans cesse la question de la confiance numérique à laquelle chacune des entreprises de l'ACN contribue activement.

Dans ce contexte, les législateurs français et européen tentent d'accorder un cadre législatif et réglementaire pensé et conçu à l'époque pré-numérique aux nouveaux paradigmes. Il en résulte pour nos professions que l'ensemble des règles qui régiront nos activités dans un futur proche sont actuellement en cours d'élaboration.

C'est pour cette raison que l'action collective et syndicale est, pour notre secteur, une nécessité impérieuse. La représentation institutionnelle de la profession, qui se trouve pour l'heure trop éparpillée pour être efficace, doit s'organiser pour pouvoir peser dans les évolutions en cours. Toutes les entreprises de la confiance numérique doivent parvenir à parler d'une seule voix sur les sujets stratégiques qui nous concernent. Telle est la mission et l'ambition que l'Assemblée Générale de l'ACN a assignée à notre association qui a entrepris un vaste mouvement visant à fédérer autour de notre structure l'ensemble des acteurs de la confiance numérique.

Cette ambition se décline tant au niveau européen, que national et régional, notamment grâce aux partenariats innovants tel que celui que nous venons de conclure avec la région Bretagne et Bretagne Développement Innovation. Cette région devient donc le premier pilote du déploiement de l'ACN en régions, d'autres suivront prochainement.

Afin de parvenir à concrétiser nos ambitions collectives, il est désormais fondamental que les entreprises du secteur s'investissent dans nos travaux et nos prises de positions. C'est pourquoi l'ACN souhaite augmenter sa visibilité auprès du secteur, via une montée en puissance sur les réseaux sociaux (Twitter et Linked In) mais également à travers une lettre d'informations dont nous avons le plaisir de vous présenter ce premier exemplaire.

L'objectif est de faire savoir, à tous les interlocuteurs de l'ACN, la nature et le contenu de nos actions de telle sorte que chaque acteur concerné puisse y participer et apporter sa contribution à l'édifice collectif qu'est notre groupement.

Nous vous en souhaitons bonne lecture.

Sommaire

Interview

Frédéric Rode, DG de BDI

Page 2

Les infos générales

Page 3

Identité numérique

Page 4

Cybersécurité

Page 5

Les actions régionales

Page 7

Veille documentaire

Page 8

**La brochure capacitaire
Cybersécurité désormais
disponible en anglais**



Voir page 3

Interview : Frédéric Rode, DG de BDI



La Bretagne est une région avec un écosystème dense d'entreprises dans le domaine de la confiance numérique (identité numérique, cybersécurité). Pouvez-vous nous présenter ce tissu régional ?

La Bretagne dispose d'un écosystème de cybersécurité dense, cohérent, historique sur les enjeux Défense, et en fort développement. La Bretagne se positionne sur 3 enjeux complémentaires : la formation, la recherche et le développement économique de la filière. Ces trois composantes contribuent à la compétitivité des acteurs de cybersécurité en accompagnant leur évolution tant sur le plan des innovations, de l'enjeu de la formation, et d'accès aux marchés applicatifs de la cybersécurité.

La composante humaine est un point clé : plus de 2800 étudiants par an bénéficient d'un cursus en cybersécurité. Plus de 80 formations sont proposées en Bretagne dans l'ensemble des écoles et universités, allant de bac + 2 à bac +5, avec des modalités de

formation initiale, continue ou en alternance.

Plus d'une vingtaine d'équipes de recherches travaillent sur des technologies de cryptographie, de détection d'intrusions et de contremesures vis-à-vis des logiciels malveillants. La Bretagne a également une expertise en protection des systèmes électroniques embarqués et coopération logiciel / matériel.

150 entreprises de cybersécurité sont recensées en Bretagne dont plus d'une cinquantaine pure-player. Au-delà de la présence des grands groupes tels que Orange Cyberdéfense, Atos ou Sopra Steria, le territoire accueille de nombreuses PME emblématiques de la filière, spécialisées en cybersécurité, identité numérique et confiance numérique.

Cet écosystème coordonné permet à la Bretagne d'être particulièrement légitime quand il s'agit de cybersécurité.

Comment la Région et BDI participent-elles à l'animation et au développement de cet écosystème ?

La transition numérique est pour la région Bretagne une priorité, et le conseil régional soutient fortement l'ensemble de l'écosystème numérique de la recherche et de l'innovation. Bretagne Développement Innovation, agence régionale de développement économique et d'innovation en entreprises, a pour mission de renforcer l'attractivité du territoire, d'anticiper et d'accélérer les transitions de l'économie régionale, avec et pour les entreprises. C'est à ce titre que BDI facilite la diffusion de technologies électronique et numérique dans les entreprises au croisement de secteurs d'activités comme l'agriculture et l'agroalimentaire ; c'est la notion « d'industrie du futur ».

Au cœur de toutes ces technologies la notion de confiance est primordiale ; cela passe par la cyber sécurité bien entendu, qui est un pôle fort en Bretagne, mais aussi par une dynamique plus globale à l'échelle nationale ; c'est à ce titre que l'accord signé entre la région Bretagne, à travers BDI, et l'ACN revêt un caractère stratégique.

Qu'attendez-vous du partenariat avec l'Alliance pour la Confiance Numérique ? Quelles synergies pouvons-nous déployer à l'avenir entre votre écosystème et notre instance de représentation institutionnelle nationale du secteur ?

Tout d'abord, il nous paraît très important de soutenir une initiative nationale structurante, car la révolution numérique doit s'appuyer sur une intensification des mesures autour de la confiance. Le partenariat avec l'ACN revêt donc à notre sens plusieurs opportunités. La première est d'intégrer une association dont le positionnement et l'ambition correspond à un besoin important de rassembler et d'agir dans l'intérêt d'une communauté et des entreprises en France et en Europe alors que les défis de souveraineté et les enjeux réglementaires sont nombreux. La veille, l'anticipation des tendances, la connaissance fine des besoins terrains pour mieux agir au global est un point que nous considérons comme majeur. Accéder à des marchés en étant plus forts à plusieurs, identifier les complémentarités des entreprises pour une offre globale, promouvoir, faire savoir et diffuser les solutions et services des entreprises, sont autant d'opportunités qui peuvent être concrétisées avec l'ACN.

Infos générales ACN



Publication de la brochure capacitaire cybersécurité

A l'occasion du Forum International de la Cybersécurité 2018 à Lille, une brochure « Cybersécurité – Approche capacitaire » a été présentée. Ce document pédagogique, édité par l'ACN, en partenariat avec la FIEEC, Le GICAT et HEXATRUST, a vocation à présenter les offres disponibles en cybersécurité. Il est destiné à toute entité s'interrogeant sur la cybersécurité : prévention, protection, réaction face à un incident... Ce document présente près de 100 offres disponibles dans ce domaine.

Le BDI devient le fer de lance de l'ACN en Bretagne

L'ACN, le Conseil régional de Bretagne et l'agence de développement économique Bretagne Développement Innovation ont signé, durant le Forum International de la Cybersécurité 2018 à Lille, une convention de partenariat. Cet accord fait de la Bretagne la 1^{ère} région pilote du déploiement de l'ACN en région et vise à échanger des informations, à mener des travaux communs et à représenter les entreprises bretonnes de la cybersécurité au sein de l'ACN, groupement professionnel qui représente la filière « Confiance numérique, identité numérique et cybersécurité » en France.

Le communiqué de presse est disponible sur le [site de l'ACN](#)

Leur site internet :



« Investing day for the European Cybersecurity »

L'ACN, en partenariat avec ECSO (European Cybersecurity Organisation) et le pôle Systematic, a organisé une journée de rencontre entre les start up et les scale up de la cybersécurité et les investisseurs intéressés par ce domaine, le 27 février à l'Espace Hamelin. Ce sont ainsi plus de 50 jeunes pousses de la cybersécurité qui ont pu exposer leur savoir-faire et pitcher devant une dizaine d'investisseurs à la recherche de projets innovants à financer.

L'ACN se dote d'une page sur Linked In

Afin de renforcer sa présence sur les réseaux sociaux, et de diffuser de manière plus régulière des messages de la profession, l'ACN vient de lancer une page Linked In. Ce nouvel outil permettra à l'ACN de relayer ses informations mais aussi de publier des tribunes et prises de positions de dirigeants d'entreprises membres, en complément des activités déjà déployées sur Twitter et sur son site Internet.

Nous suivre sur Linked In.

Ils ont rejoint l'ACN récemment :



Identité numérique



Le Gouvernement relance le projet "Identité Numérique"

Le 5 janvier 2018 a eu lieu une réunion entre Gérard Collomb, ministre de l'Intérieur, Nicole Belloubet, Garde des Sceaux, et Mounir Mahjoubi, secrétaire d'Etat chargé du numérique dans le cadre d'un comité d'orientation stratégique afin de déterminer les étapes des travaux à venir pour mettre en place des solutions d'identité numérique. Ils ont ainsi signé une lettre de mission adressée à Valérie Peneau, inspectrice générale de l'administration, qui va diriger l'équipe interministérielle chargée de conduire ce programme, dont les travaux commencent dès le début de cette année.

Les transactions publiques ou privées entre usagers, entreprises ou associations sont de plus en plus dématérialisées, ce qui nécessite une identification. Ainsi, une identification numérique permet à chacun de justifier de son identité de manière sécurisée, accessible et économique, que ce soit dans le cadre d'échanges avec l'administration que de transactions privées, par exemple lors d'achats sur internet.

Cette identification numérique sécurisée sera ouverte à l'ensemble des acteurs du numérique qui souhaitent en bénéficier, pour simplifier et améliorer la sécurité de la vie numérique, tout en préservant l'identité des utilisateurs et en luttant contre la fraude.

L'ouverture de ce nouveau service public devra être faite à la rentrée 2019, selon le calendrier arrêté par le Premier Ministre.

Tous les acteurs concernés seront associés à ce projet, afin d'aborder toutes les questions techniques, juridiques, éthiques, organisationnelles et financières soulevées par la mise en place d'un parcours d'identification numérique sécurisée, dans un processus de concertation transparent et ouvert.

L'ACN sera prochainement auditionnée par Valérie Peneau afin d'exprimer la position de la profession.

Lancement d'un groupe de travail ACN-ANTS sur l'e-Passeport

Une convention de partenariat portant sur la mise en place et la gestion d'un groupe de Travail *ad hoc* relatif au "e-Passeport" afin de définir les actions à entreprendre pour parvenir à couvrir l'intégralité des problématiques de conformité de l'e-Passeport au regard de la norme ICAO 9303.

Ce groupe de travail devra notamment rédiger :

- Un document de travail qui présentera les objectifs, les moyens, l'approche et le planning ;
- Une « job card » qui reprendra la liste des actions à conduire pour atteindre les objectifs définis ;
- Une analyse d'impact qui évaluera les incidences sur l'existant.

Les travaux du groupe de travail pourront avoir lieu dans les locaux de l'ACN ou de l'ANTS.

Les travaux du groupe de travail devront s'inscrire dans le calendrier des travaux de normalisation suivis par l'ANTS et respecter, notamment, les échéances suivantes :

- Juin 2018 : 1^{ère} version des documents précités
- Décembre 2018 : un rapport de présentations des écarts de conformité du « e-Passeport » au regard de la norme ICAO 9303.
- Mars 2019 : un rapport reprenant l'ensemble des propositions de couverture des écarts de conformités du « e-Passeport » au regard de la norme ICAO 9303.



Agence Nationale des Titres Sécurisés

Cybersécurité



European Cyber Act

La Commission européenne a proposé, le 13 septembre dernier, un projet de règlement qui ambitionne de redéfinir le mandat et le rôle de l'ENISA et propose de créer un nouveau schéma européen de certification en matière de cybersécurité.

Dès la présentation de ce texte, notre profession s'est organisée autour de l'ACN et notamment de son GT2 pour analyser cette proposition et construire une réponse commune, en lien avec l'ANSSI. Une position a ainsi pu être très rapidement publiée et nous a permis de sensibiliser les décideurs politiques nationaux à ce sujet stratégique majeur.

Le European Cyber Act est désormais dans sa phase législative : le Parlement européen examine actuellement en commission ce texte. Là encore, l'ACN a été extrêmement présente et nous avons formulé de nombreux amendements (voir ci-dessous) transmis à tous les députés européens concernés.

En dépit de ces actions fortes, le texte comporte encore de nombreuses incertitudes, notamment quant à la définition des niveaux de certification, à la participation des industriels à l'élaboration des schémas de certification et aux garanties d'homogénéité et de sécurité dans la mise en œuvre de ce texte.

Il est essentiel que notre profession demeure mobilisée pour porter nos messages et nos amendements et peser sur ce texte qui façonnera le cadre d'action de toutes les entreprises du secteur dans les années à venir.

Cyber Act : ACN auditionné au Sénat

Alexis Caurette, Président du GT2 Cybersécurité de l'ACN, a été auditionné par les sénateurs Laurence Harribey et René Danési sur le European Cybersecurity Act. Après avoir examiné ce texte, en octobre, au regard de la subsidiarité (avis sur lequel l'ACN avait déjà été auditionnée), la Commission des Affaires européennes du Sénat se concentre cette fois sur le fond et devrait émettre ses recommandations dans le courant du mois d'avril.

Amendements ACN au Parlement européen

L'ACN a été très active dans le parcours législatif du European Cyber Act, en portant plus de 20 amendements à la connaissance des députés européens dans les commissions pertinentes (ITRE, IMCO, LIBE). Ces amendements visent principalement à conserver les acquis stratégiques de la certification, à clarifier les process de certification et à s'assurer de l'homogénéité de la mise en œuvre de cette réglementation.

Event CyberTaskForce

Les membres de la CyberTaskForce se sont réunis lundi dernier, 19 mars 2018, à l'occasion d'une réunion de travail autour de Mounir Mahjoubi, secrétaire d'État chargé du Numérique.

En présence d'une dizaine de parlementaires présidents de groupe d'études, du ministère des Armées, du ministère de l'Intérieur et de la CNIL, dirigeants des PME et représentants professionnels de la cyber ont pu apporter leur contribution aux débats du projet de loi PACTE.

Le ministre a demandé à la CyberTaskForce de poursuivre ses travaux sur des enjeux identifiés et de lui formuler des recommandations dans les prochaines semaines.



Les actions régionales



La Bretagne



BreizhCTF : 24h dédiées à la sécurité informatique

Conçu par des membres de la team Hexpresso et organisé par BDI

Avec 300 participants, la 4ème édition du BreizhCTF est désormais un événement bien ancré dans le paysage des compétitions de sécurité informatique.

3 temps forts au BreizhCTF : des workshops destinés à des professionnels de la sécurité informatique qui pratiquent en petit comité des enjeux de cybersécurité ; des sessions de rumps : 5 minutes pour partager avec la communauté des sujets, défis relevés, astuces ; la nuit de compétition en équipe de 5.

Le BreizhCTF est ouvert à tous : professionnels, étudiants, débutants, confirmés, passionnés, curieux.

Le but du BreizhCTF est de permettre, sur une journée et une nuit, le partage et la rencontre autour des thématiques associées à la sécurité des systèmes d'information. Le BreizhCTF est une manifestation où les personnes techniques et non-techniques peuvent se rencontrer et partager librement toutes sortes d'informations.

BreizhCTF – 20-21 avril 2018 – Rennes

www.breizhctf.com

Intereg CYBER

Objectif : améliorer les politiques publiques de soutien à la compétitivité des PME qui travaillent dans le domaine de la cybersécurité. CYBER regroupe 7 régions et pays européens : Bretagne (BDI + Région), Castilla y Leon (ES), Toscane (IT), Wallonie (BE), Slovaquie, Slovaquie e Estonie. ECSO, l'organisation européenne de la cybersécurité, participe également au projet en tant que Advisory partner.

Sous la coordination de BDI, les partenaires échangeront des bonnes pratiques et définiront des plans d'action régionaux pour mettre en place des mesures de soutien plus efficaces et assurer une meilleure gestion et utilisation des fonds FEDER à destination des entreprises de la cybersécurité.

Avec un budget total d'1.8M€, le projet aura une durée de 5 ans.

La région PACA



Le projet de R&D PadDOC, labellisé par le Pôle SCS et financé en 2013 par le FUI16 permet la création d'une nouvelle norme en 2018 dans l'échange sécurisé de données.

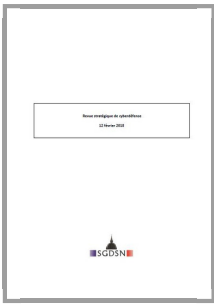
Le projet mené par 2 PME de la région PACA, ABC Smartcard et Anyces, 1 grand groupe Docapost et le laboratoire de Sophia Antipolis, I3S, portait sur la dématérialisation du contenu de nos sacs à main et sacs en mettant sous contrôle du porteur l'ensemble de ses données pour réaliser des formalités publiques et privées en un seul « tap » sur son téléphone mobile.

Cette nouvelle norme dite « expérimentale » présente une solution ouverte et intégrable conforme au Règlement Général européen sur la Protection des Données (RGPD) qui entrera en vigueur en mai 2018.

Pour en savoir plus, [**cliquez ici**](#).

Veille documentaire

La revue stratégique de cyberdéfense

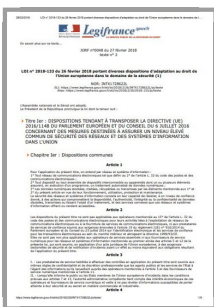


Secrétariat Général de la Défense et de la Sécurité Nationale - 14 février 2018

Le SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale) a publié, le 14 février 2018, un véritable Livre blanc de la cyberdéfense, rédigé par Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

Organisée en trois parties, cette revue présente une vue d'ensemble de la cybermenace, avant de proposer des solutions pour améliorer la cybersécurité en France. Il est nécessaire de protéger les systèmes d'information de l'Etat, des organismes d'importance vitale, mais également renforcer la sécurité numérique pour les institutions, les collectivités mais également les citoyens.

Loi de transposition de la directive NIS



Parlement - 26 février 2018

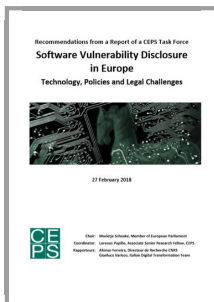
Le projet de loi transposant la directive 2016/1148 du 6 juillet 2016 (directive NIS), présenté au Sénat par le secrétaire d'Etat au Numérique, Mounir Mahjoubi, a été adopté le 26 février 2018.

Cette loi vise les Opérateurs d'Importance Vitale (OIV) ainsi que des acteurs publics et privés afin que ceux-ci améliorent la protection de leurs systèmes d'information.

Disponible [ici](#)

CEPS Task Force Software Vulnerability Disclosure in Europe

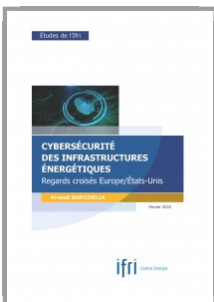
Center for European Policy Study - février 2018



Le CEPS demande à la Commission européenne et aux Etats membres d'établir une proposition légale, complétée par des législations nationales couvrant ce processus, afin d'avoir une clarification sur la découverte et la divulgation des vulnérabilités, et il recommande que les centres d'alerte et de réaction aux attaques informatiques encadrent également ce processus. Ces cadres doivent être annoncés sur les sites internet des organisations qui proposent de dénoncer les vulnérabilités, et que les chercheurs peuvent consulter et utiliser pour leur sécurité juridique.

Cybersécurité des infrastructures énergétiques, regards croisés Europe/USA

Institut Français des Relations Internationales - février 2018



Au cours des dernières années, l'UE et les États-Unis ont progressivement adopté une série de mesures et de réglementations pour protéger les infrastructures énergétiques face au risque cyber. Cependant, les approches américaines et européennes présentent de nombreuses différences.

Proposition de règlement e-Privacy

Commission européenne - mars 2018



La Commission européenne a présenté en janvier 2017 une proposition de règlement COM(2017) 10 final concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (dit « e-Privacy »), actualisée le 22 mars 2018 par la Présidence du Conseil de l'UE concernant la protection des informations stockées dans les équipements terminaux des utilisateurs finaux, les informations à fournir et options à proposer pour les paramètres de confidentialité, et les annuaires accessibles au public.

<https://www.confiance-numerique.fr>



Twitter
@ACN_SecNum



Linkedin
ACN - Alliance pour la
Confiance Numérique