Contacts Presse :

Raphaël Soudan +33 1 53 32 55 17
raphael.soudan@ketchum.fr

Bastien Rousseau +33 1 56 02 35 05
bastien.rousseau@ketchum.fr

Une étude BSA | The Software Alliance concernant les lois relatives à la cybersécurité dans l'UE révèle des écarts de niveau de préparation entre les Etats membres

Bruxelles — 3 mars 2015 — Une toute première analyse des lois et règles de cybersécurité au sein de l'Union Européenne révèle des écarts de niveau de préparation et une certaine fragmentation entre les Etats membres.

Dans ce rapport rendu public aujourd'hui, BSA | The Software Alliance évalue les lois, règles et politiques nationales des 28 Etats membres de l'UE au regard de 25 critères jugés essentiels pour lutter efficacement contre la cybercriminalité. L'objectif est de proposer des mesures formelles aux Etats membres de l'UE pour leur permettre à la fois d'évaluer objectivement leur politique nationale et aussi d'y trouver des orientations pour renforcer leur arsenal juridique en faveur de la cybersécurité.

« Les mesures de protection contre la cybercriminalité ne sont pas uniformes dans toute l'Europe. Et même si la plupart des Etats membres s'accordent à considérer la cybersécurité comme une priorité, des incohérences d'approche créent des vulnérabilités qui exposent le Marché unique aux menaces », explique Thomas Boué, Directeur Règlementation au sein de la BSA pour la zone EMEA. *« La Directive concernant la sécurité des réseaux et de l'information pourrait aider à poser des bases communes plus solides en faveur de la cybersécurité et de la cyber résilience ; mais il est nécessaire pour cela d'uniformiser les efforts de préparation de l'infrastructure la plus critique en Europe et d'introduire des processus harmonisés de reporting et de partage de l'information au sein du Marché unique. »*

Voici quelques-unes des conclusions du rapport :

- La plupart des Etats membres de l'UE voient la cybersécurité comme une priorité nationale, surtout au regard de l'infrastructure critique.
- Des décalages importants existent entre les règles de cybersécurité, les instruments juridiques et les capacités opérationnelles des Etats membres, qui créent des brèches majeures dans la barrière de protection contre la cybercriminalité en Europe.
- Quasiment tous les Etats membres de l'UE se sont dotés d'équipes d'intervention en cas d'incident mettant à mal la cybersécurité ; toutefois, la mission et l'expérience de ces équipes demeurent variables.
- L'insuffisance de coopération systématique public-privé est inquiétante, de même que la collaboration des gouvernements de l'UE, des entités non-gouvernementales et des partenaires internationaux autour de la question de la cybersécurité.
- Le rapport montre que la France dispose d'une stratégie nationale de cybersécurité depuis 2011, même si celle-ci se focalise surtout sur la défense et la sécurité nationale. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est une autorité officielle dédiée à

la sécurité informatique, intégrée au Centre d'alerte et de réaction aux attaques informatiques français, le CERT-FR (Computer Emergency Response Team). La stratégie de cybersécurité en place préconise une coopération plus étroite avec le secteur privé, mais les développements en ce sens sont insuffisants à ce jour. L'ANSSI publie des mesures de sécurité spécifiques à certains secteurs ce qui fait de la France l'un des rares pays de l'UE à avoir adopté une approche aussi ciblée de la gestion de la cybersécurité.

Le rapport encourage les Etats membres de l'UE à se concentrer sur les quatre éléments clés d'un cadre juridique fort de protection de la cybersécurité :

- Mettre en place et actualiser un cadre juridique et réglementaire basé sur une stratégie de cybersécurité nationale complétée par des plans de cybersécurité sectoriels,
- Constituer des entités opérationnelles aux responsabilités clairement établies concernant la sécurité informatique opérationnelle, les interventions d'urgence et en cas d'incident,
- Promouvoir la confiance et le travail en partenariat avec le secteur privé, les ONG et les partenaires et alliés internationaux,
- Renforcer les mesures d'éducation et d'information sur les risques et les priorités de lutte contre la cybercriminalité.

Dans le même temps, le rapport prévient les gouvernements européens de se méfier des régimes protectionnistes contre-productifs qui risquent de freiner la lutte contre la cybercriminalité plutôt que de la soutenir. Plus spécifiquement, les Etats membres ont intérêt à :

- Eviter les prescriptions inutiles ou déraisonnables qui risquent de limiter les choix et de faire grimper les coûts, et notamment les demandes de test ou de certification uniques ou spécifiques au pays ; les obligations liées aux contenus locaux ; les contraintes de divulgation d'informations sensibles, comme le code source ou les clés de chiffrement ; et les limitations des droits de propriété intellectuelle pour les étrangers,
- Promouvoir les standards techniques prescrits par l'industrie et reconnus internationalement plutôt que de chercher à les manipuler,
- Eviter les règles de localisation des données et faciliter la libre-circulation des données entre les marchés,
- Eviter les technologies indigènes qui entravent la concurrence étrangère et pénalisent l'innovation mondiale.

Le rapport de synthèse pour les 28 pays ainsi que les fiches détaillées pour chaque Etat membre de l'UE sont disponibles sur : www.bsa.org/EUcybersecurity

A propos de BSA | The Software Alliance

BSA | The Software Alliance (www.bsa.org) est le premier défenseur des intérêts de l'industrie logicielle auprès des autorités gouvernementales et des places de marché internationales. Cette association réunit des entreprises d'envergure internationale, à l'origine de solutions logicielles innovantes qui contribuent à l'essor économique et améliorent la qualité de vie. Basée à Washington DC et présente dans une soixantaine de pays, la BSA propose de nouveaux programmes de conformité prônant l'usage légal des logiciels et promeut les politiques publiques à même de favoriser l'innovation technologique et de stimuler l'essor de l'économie numérique.