BSA The Software Alliance

Tableau de bord de la cybersécurité dans l'UE

Vers un cyberespace européen sécurisé

galexia

CONTENU

RÉSUME EXÉCUTIF

Les promesses de notre monde interconnecté sont impossibles à mesurer. La technologie fait dorénavant partie de quasiment tous les secteurs de l'économie mondialisée, ceux des services bancaires, des télécommunications, de la fourniture d'électricité, etc. Mais les avantages promis s'accompagnent de menaces tout aussi réelles.

Les criminels, toujours plus nombreux et ayant accès à des technologies de pointes, voient dans la promesse de notre monde connecté de nouvelles opportunités de s'enrichir par le vol ou de tirer profit de failles et de vulnérabilités pour perturber ou détruire leurs cibles. Malheureusement, la courbe de l'exposition aux menaces suit celle de la multiplication des avantages offerts par la technologie. Contrer ces menaces et renforcer la résilience de nos systèmes connectés suppose une bonne dose de flexibilité et une forte volonté d'évolution.

Pour les États, les moyens de lutte contre les cyber attaques (et la capacité d'atténuer leurs effets néfastes et d'identifier les menaces émergentes) se trouvent dans les règles de cybersécurité qu'ils adoptent et font appliquer. Trois éléments doivent être réunis : les cadres juridiques et réglementaires appropriés, la participation du public et l'infrastructure nécessaire pour mettre en œuvre les cadres.

Les lois, règles, institutions et la structure nécessaire pour faciliter la coopération avec les différents interlocuteurs sont les bases essentielles dont les États et les organisations non gouvernementales ont besoin pour protéger leurs systèmes, prévenir et réduire les cyber attaques et réagir en conséquence le cas échéant.

De tels cadres juridiques et réglementaires et les structures de mise en œuvre appropriées doivent être stables et sans ambiguïté, mais ils doivent aussi préserver un niveau suffisant de flexibilité. Il faut notamment qu'ils tiennent compte du contexte changeant des menaces, caractéristique de l'univers technologique, et qu'ils puissent être adaptés.

L'objet de ce rapport, le premier tableau de bord de la cybersécurité dans l'UE réalisé par la BSA, est de donner les moyens aux officiels de l'état de chaque Etat membre de l'UE d'évaluer les règles en vigueur dans leur pays au regard des critères et mesures et de se comparer à leurs voisins européens.

Voici une synthèse des conclusions les plus importantes du rapport :

- La plupart des états membres de l'UE s'accordent sur le fait qu'ils devraient considérer comme une priorité nationale importante les efforts en matière de cybersécurité et de cyber résilience, avec une attention particulière portée à la protection des infrastructures critiques.
- Des décalages importants existent entre les règles de cybersécurité, les instruments juridiques et les capacités opérationnelles des États membres, qui créent des brèches majeures dans la barrière de protection contre la cybercriminalité en Europe.
- 27 États membres de l'UE ont constitué des entités opérationnelles, du type du centre national d'alerte et de réaction aux attaques informatiques, CERT (computer emergency response team), mais les missions et les degrés d'expérience de ces entités sont très variables.

Pour plus d'information sur la méthodologie utilisée, rendez-vous sur le site : www.bsa.org/EUcybersecurity.

- La coopération systématique avec des entités non-gouvernementales est insuffisante, de même que les partenariats public-privé : seuls cinq États membres de l'UE ont mis en place des règles d'encadrement de ces partenariats. Il reste donc beaucoup à faire pour instaurer une collaboration efficace et volontariste entre les États et le secteur privé qui possède et exploite la majorité des services commerciaux liés aux infrastructures critiques en Europe.
- Il reste de gros efforts à faire avant d'aboutir à une approche cohérente et à une ligne directrice commune de la cybersécurité dans l'UE. La Directive concernant la sécurité des réseaux et de l'information et son application sont l'occasion de jeter un coup de projecteur sur la protection des actifs et des services les plus critiques des États membres. Cette Directive pourrait jouer un rôle clé pour combler les lacunes de cybersécurité en Europe.

Le rapport de cette année souligne les principales difficultés et les améliorations possibles pour la cybersécurité dans l'UE. Il faudrait que les États membres alignent leurs approches de la cybersécurité et qu'ils accordent leurs capacités sur une ligne directrice comparable et cohérente pour pouvoir envisager un vrai marché unique du numérique dans l'UE.

La cybersécurité et la cyber résilience sont souvent envisagées sous l'angle du financement, or ces questions relèvent surtout de décisions de la direction. Mettre en place les règles nécessaire et les cadres juridiques et opérationnels appropriés, améliorer la collaboration avec les différents interlocuteurs concernés, partager des informations pertinentes et utiles sur la cybersécurité et donner la priorité à la protection des infrastructures critiques, telles sont les étapes qui vont permettre de renforcer la cybersécurité et la cyber résilience de tous les États membres de l'UE.

En plus de ce rapport, les réponses détaillées obtenues sont consultables en ligne sur : www.bsa.org/EUcybersecurity.

La cybersécurité étant un domaine en perpétuelle évolution, ce rapport a vocation à évoluer. Le site Web sera constamment mis à jour en fonction des décisions prises par les États et les décideurs nationaux pour combler les manques identifiées dans les différents domaines. Nous vous invitons à prendre connaissance des résultats et à communiquer à la BSA | The Software Alliance toute information utile concernant des changements.

MÉTHODOLOGIE

Cette étude de la maturité des politiques de cybersécurité a porté sur l'évaluation de 25 critères répartis dans cinq thèmes principaux. (voir les résultats, pages 8–9.) Pour chaque critère, les réponses correspondent au statut Oui, Non, Partiellement ou Ne s'applique pas. Aucun classement général ni score total n'est proposé pour cette étude.

Cette analyse est le fruit de recherches menées isolément à partir d'informations publiques librement disponibles, sans interroger directement les agences nationales. Chaque fois que possible, des liens vers des ressources et compléments d'information sont proposés. Ils figurent sur notre page d'accueil.

La période de recherche a pris fin le 1er janvier 2015 et les informations du rapport sont correctes à cette date.

Pour plus d'information sur la méthodologie utilisée, rendez-vous sur le site : www.bsa.org/EUcybersecurity.

LES CONDITIONS D'UN CADRE JURIDIQUE SOLIDE POUR LA CYBERSÉCURITÉ

Construire des bases juridiques solides

Les États doivent se donner les moyens de constituer un cadre juridique et réglementaire complet et de le tenir à jour, en s'appuyant sur une stratégie nationale solide de cybersécurité. Ce cadre doit idéalement reposer sur les principes clés suivants.

- **Être basé sur les risques et être jugé prioritaire :** les cybermenaces prennent diverses formes, sont de magnitudes différentes et avec des degrés de gravité plus ou moins importants. Il est bon de commencer par établir une hiérarchie des priorités, sur la base d'une analyse des risques objective, en plaçant en haut les actifs critiques et/ou les secteurs critiques, de façon à concentrer les moyens de cyberprotection là où le potentiel de préjudice est le plus fort.
- **Être neutre technologiquement :** une approche technologiquement neutre de la cybersécurité est vitale pour pouvoir sélectionner les solutions les plus sûres et les plus efficaces actuellement sur le marché. Les règles ou contraintes spécifiques qui obligent à utiliser telle technologie compliquent l'adoption de contrôles de sécurité évolutifs et des meilleures pratiques émergente avec le risque de créer des points uniques de défaillance.
- **Être pratique :** une stratégie n'est efficace que si elle peut être adoptée par le plus grand groupe possible d'actifs critiques et mise en œuvre au profit de l'échelle la plus large d'acteurs critiques. La supervision excessivement contraignante des opérateurs privés par l'Etat ou l'intervention excessivement intrusive des réglementations dans leur gestion opérationnelle des risques de cybersécurité peut s'avérer contreproductive, dès lors que l'attention et le temps que les ressources devraient consacrer à l'efficacité de protection sont mobilisés par de multiples contrôles de conformité administrative.
- **Être flexible :** la gestion des cyber risques est une fonction multidisciplinaire et il n'existe pas de recette miracle. Chaque industrie, chaque système et chaque activité sont confrontés à des enjeux différents et les différents acteurs doivent bénéficier de suffisamment de flexibilité pour satisfaire leurs propres besoins.
- **Respect de la vie privée et des libertés civiles :** il faut trouver un juste équilibre entre les besoins de sécurité et la nécessité de protéger la vie privée et les libertés civiles. Il est important de veiller à la juste proportion entre les besoins et les obligations, sans faire reculer les droits fondamentaux, de suivre une procédure équitable et d'établir une supervision judiciaire appropriée.

Constituer des entités opérationnelles aux responsabilités clairement définies en matière de sécurité

Les États devraient mettre en place des entités opérationnelles pour faciliter la prévention des incidents de cybersécurité et développer une capacité de réaction le cas échéant. Ces équipes opérationnelles doivent être spécialistes de la sécurité informatique, des interventions d'urgence et de la gestion des incidents.

Instaurer la confiance et travailler en partenariats

Aucun pays, ni aucun gouvernement ne peut gérer isolément les risques de cybersécurité. La collaboration avec des entités non-gouvernementales et avec des alliés et partenaires internationaux est un composant crucial d'une approche efficace de la cybersécurité.

- **Approche de partenariat avec le secteur privé :** les infrastructures étant majoritairement détenues par le secteur privé, il est essentiel d'entretenir la coopération public-privé. Cette coopération contribue également à l'efficacité de gestion des risques en favorisant le partage d'information, d'expérience et des points de vue de multiples sources. Des efforts particuliers sont nécessaires pour éviter les obstacles légaux qui risquent d'entraver la confiance.
- **Lutte contre l'isolement avec un positionnement global et ouvert :** les cyber menaces étant globales, pour que les règles et stratégies de cybersécurité soient efficaces, il faut miser sur une vision internationale et sur la mise en commun des efforts avec ceux des partenaires et des alliés. Il est également recommandé de privilégier l'adhésion volontaire à des normes technologiques internationales et guidées par le marché pour favoriser le partage d'information et la protection à tous les niveaux.

Renforcer les mesures éducatives et d'information sur les risques liés à la cybercriminalité

Les individus, les processus et la technologie sont tout aussi importants pour assurer la cybersécurité. Même la meilleure technologie ne donnera pas de résultats satisfaisants si elle est mal utilisée. Les efforts de sensibilisation, d'éducation et de formation portant sur les priorités clairement articulées de cybersécurité, les principes, les règles, les processus et les programmes sont des composants essentiels de toute stratégie de cybersécurité.

PRINCIPALES CONCLUSIONS

Des incidents liés à la cybersécurité ont été largement médiatisés récemment et soulignent l'importance cruciale de renforcer la cyber résilience en général, et la protection des infrastructures critiques contre les cybermenaces, en Europe et dans le monde. Pour atteindre ces objectifs, les acteurs concernés du public et du privé doivent pouvoir prévenir et limiter les cyber-attaques et réagir en conséquence en cas d'incident.

Alors que la volonté de renforcer la cyber résilience existe dans les États membres et au niveau de l'UE, ce rapport, le premier tableau de bord de la cybersécurité dans l'UE, dresse un état des lieux complet des équipements et des capacités actuellement disponibles en matière de cybersécurité.

Comme détaillé plus bas, le rapport analyse les règles et politiques de cybersécurité dans les États membres de l'UE suivant cinq grandes thématiques :

- les bases légales de la cybersécurité ;
- les capacités opérationnelles ;
- les partenariats public-privé ;
- les plans de cybersécurité sectoriels ;
- l'éducation.

LES BASES LÉGALES

Les législateurs ont un rôle essentiel à jouer pour faire en sorte que les entités du public et du privé aient les capacités qu'il leur faut pour relever les défis que pose la cybersécurité dans notre monde toujours plus connecté. Ils peuvent procéder en faisant appliquer les cadres légaux et réglementaires appropriés, mais aussi en insistant sur la nécessité de sensibiliser aux enjeux de cybersécurité et de la coopération des différents acteurs concernés de façon à concerter les efforts de renforcement de la cyber résilience.

Un composant clé et, à bien des égards, le socle même de ce cadre consiste en une stratégie nationale de cybersécurité, incontournable pour gérer les cyber risques à l'échelle nationale et pour développer une législation appropriée pour soutenir ces efforts. Idéalement, une stratégie de cybersécurité doit être un « document vivant », développé et mis en œuvre en partenariat avec les principaux interlocuteurs concernés du public et du privé. Ce document doit établir les principes clairement articulés et les priorités qui reflètent les valeurs de la société, les traditions et les principes de justice.

A cet égard, un effort d'amélioration est nécessaire dans l'UE. Seuls 19 des 28 États membres ont mis en place des stratégies de cybersécurité plus ou moins détaillées et complètes, et 8 états n'ont aucun cadre en ce sens. Même dans le cas des pays ayant adopté des stratégies de cybersécurité, la qualité de celles-ci est variable, les clauses restent vagues et généralistes, sans véritable plan d'implémentation.

De surcroît, la plupart de ces documents restent « statiques ». Seul un petit nombre de pays a déjà révisé et amélioré ses stratégies initiales et publié des mises à jour. Une minorité seulement des États membres a renforcé sa stratégie de cybersécurité avec des instruments réglementaires et législatifs préconisant des obligations de sécurité, de classification des informations et de protection des infrastructures critiques.

Les gouvernements devraient évaluer et définir clairement les priorités de protection des infrastructures et des services critiques. Tous les actifs, systèmes, réseaux, données et services ne sont pas sur le même niveau. Les décideurs doivent mesurer l'importance d'évaluer les infrastructures nationales, en fonction de critères objectifs et en tenant compte des suggestions publiques pour déterminer les services et les fonctions les plus

Les législateurs ont un rôle essentiel à jouer pour faire en sorte que les entités du public et du privé aient les capacités qu'il leur faut pour relever les défis que pose la cybersécurité dans notre monde toujours plus connecté.

critiques, qui s'ils étaient détruits ou compromis par un incident de cybersécurité pourraient avoir une portée nationale.

Les conclusions de cette étude montrent que plus de la moitié des États membres de l'UE n'ont pas encore évalué les conditions d'une future stratégie ou d'un plan de protection de leurs actifs les plus importants.

Une fois que ces infrastructures critiques sont identifiées, il reste à évaluer leur cyber résilience pour identifier les vulnérabilités et écarts et y remédier.

Les meilleures pratiques développées dans le secteur privé comprennent souvent des audits systématiques internes et de tiers pour tester la cyber résilience des systèmes critiques. Cette approche est aussi utile pour le secteur public, mais l'étude a montré que la plupart des États membres de l'UE et des organes publics n'observent pas les meilleures pratiques recommandées.

Enfin, dans le contexte de l'intensification des débats au sujet du signalement obligatoire des cyber incidents, il est important de noter que **la plupart des pays européens s'opposent à ces systèmes, et qu'ils préconisent plutôt la coopération formelle ou informelle avec le secteur privé.** Beaucoup craignent que l'obligation de notifier les incidents soit moins efficace que l'échange d'information sur la base de la confiance mutuelle et d'une collaboration poursuivie.

Si un régime de notification devait être introduit, la plupart des États membres s'accordent sur le fait que seuls les incidents ayant un impact significatif ou exposant à un risque sérieux doivent être concernés par l'obligation.

Il ne fait aucun doute que la diffusion de l'information sur la question de la cybersécurité est un aspect important d'une approche efficace de cyber résilience, qui serve les intérêts publics et privés. C'est la condition de la sensibilisation du plus grand nombre, permettant à chaque personne concernée d'adapter sa posture de sécurité en fonction de l'évolution des menaces.

L'efficacité de partage de l'information suppose que l'information soit protégée et appelle donc au respect de règles adaptées de classification. La plupart des États membres s'accordent sur ce point et ont quasiment tous mis en place des règles de classification.

Les gouvernements devraient encourager le partage de l'information en favorisant la création de partenariats public-privé et la collaboration sectorielle (voir plus bas), et en mettant à disposition les ressources humaines et techniques nécessaires, les entités opérationnelles et les protections légales appropriées encadrant les responsabilités excessives et les risques de demandes de réparation. Ils devraient également identifier et apporter une réponse à chaque obstacle juridique et réglementaire freinant le partage de l'information.

ENTITÉS OPÉRATIONNELLES

Il convient d'établir des capacités de réaction aux incidents pour gérer les événements les plus critiques et significatifs qui menacent la confidentialité, l'intégrité ou la disponibilité des systèmes et réseaux d'information importants. Les centres d'alerte et de réaction aux attaques informatiques, CERT ou CSIRT (computer security incident response teams) peuvent jouer un rôle crucial dans l'amélioration de la cyber résilience.

Ces organes peuvent apporter leur concours aux victimes d'attaques pour réagir en cas d'incident ; donner accès aux informations concernant les vulnérabilités et les menaces aux principaux représentants de l'Etat, du secteur privé et selon le cas au grand public ; et ils peuvent proposer des suggestions d'amélioration de la sécurité informatique et des réseaux.

C'est donc une bonne chose que la plupart des États membres de l'UE aient mis en place des centres CERT, et qu'il ne reste plus qu'à Chypre et à l'Irlande de rendre leur CERT opérationnel.

L'efficacité du partenariat entre les secteurs public et privé est d'autant plus importante que nombre d'entités non-gouvernementales gèrent et exploitent les infrastructures critiques dont nous dépendons au quotidien, y compris celles qui contrôlent les transports, la santé, la banque et l'énergie.

La plupart des pays ont aussi constitué des autorités nationales compétentes en charge de la sécurité des systèmes informatiques et des réseaux.

PARTENARIATS PUBLIC-PRIVÉ

La culture de la cybersécurité requiert des efforts collaboratifs et la coordination de tous les publics concernés à l'échelle nationale. L'efficacité du partenariat entre les secteurs public et privé est d'autant plus importante que nombre d'entités non-gouvernementales gèrent et exploitent les infrastructures critiques dont nous dépendons au quotidien, y compris celles qui contrôlent les transports, la santé, la banque et l'énergie.

L'importance de la coopération a beau être reconnue en Europe, il existe une grande diversité d'approches nationales et de niveaux de maturité sur cette question. Cinq pays, l'Autriche, l'Allemagne, les Pays-Bas, l'Espagne et le Royaume-Uni, montrent l'exemple en termes de partenariats public-privé pour la cybersécurité.

Dans la majorité des autres États membres, les partenariats public-privé pour la cybersécurité sont inexistants, très limités ou à un stade de développement très peu avancé.

PLANS DE CYBERSÉCURITÉ SECTORIELS

Certain éléments de la protection de la cybersécurité s'appliquent de façon générale et globale, et les organisations nationales et internationales émettent de très nombreuses recommandations, mais certaines entités commerciales ont besoin d'orientations spécifiques tenant compte de leurs particularités ou qu'on leur suggère des méthodes adaptées aux risques ou aux opérations propres à leur secteur d'activité.

De plus, malgré l'intérêt croissant en faveur de réponses sectorielles aux menaces pour la cybersécurité, les efforts d'implémentation pratique restent relativement limités dans les États membres. Les mêmes pays chefs de file des partenariats public-privé sont les leaders dans ce domaine ; ils préconisent le plus souvent le dialogue et les échanges d'informations propres à chaque secteur avec les représentants du secteur privé. Il serait bon que chaque secteur puisse être conseillé pour faire de même.

ÉDUCATION

Aucune entité individuelle, ni aucun groupe d'intérêt ne peut garantir seul la sécurité du cyberespace et aucun individu, ni aucun groupe ne peut s'exonérer de responsabilité vis-à-vis de la cybersécurité. Si les États, les organisations de toutes tailles et les consommateurs doivent tous prendre des mesures pour sécuriser leurs propres systèmes, il ne faut pas négliger le rôle crucial de l'éducation et de la sensibilisation.

Ceci suppose de mettre en place des campagnes d'éducation et de sensibilisation et de faciliter les formations aux questions de cybersécurité dans les universités et plus tôt dans les cursus scolaires.

L'Union européenne exprime sa forte volonté d'éducation et de sensibilisation aux questions de cybersécurité et prend des mesures en ce sens. A titre d'exemple, le mois de la cybersécurité en Europe se tient chaque mois d'octobre et la plupart des pays de l'UE participent.

D'un autre côté, un petit nombre de pays, dont la Grèce, Malte, le Portugal et la Slovénie, doivent encore mettre en place des stratégies d'éducation nationales sur cette problématique.

LES ÉCUEILS SUR LE CHEMIN VERS LA SECURITÉ

Certains États invoquent la cybersécurité comme justification de l'adoption de règles qui vont au-delà du strict nécessaire pour répondre aux préoccupations de sécurité légitimes. Souvent, de telles règles pénalisent la cybersécurité plus qu'elles l'améliorent. Elles imposent aussi des barrières abusives aux producteurs et fournisseurs de services mondiaux pour l'accès aux marchés, que ces barrières soient délibérées ou non.

Éviter les obligations inutiles ou déraisonnables

Une politique de cybersécurité appropriée doit permettre aux organisations de développer et d'adopter le plus large choix possible de solutions de cybersécurité de pointe. Elle doit également permettre aux entités d'appliquer des mesures de sécurité les plus efficaces possible pour contrer les risques spécifiques auxquels elles sont exposées.

Certains États imposent au contraire diverses obligations qui ont pour effets de restreindre le choix, d'accroître les coûts et d'empêcher l'utilisation des outils de cybersécurité les mieux adaptés. Il s'agit, entre autres, de conditions de certification spécifiques à un pays ou d'obligations locales de test ; de demandes d'adaptation des contenus dans la langue locale ; d'obligations de révélation d'informations sensibles, comme le code source et les clés de chiffrement ; ou encore de limitations des droits de propriété intellectuelle pour les étrangers.

Ne pas manipuler les standards

Les standards technologiques jouent un rôle vital dans la mise en oeuvre et le renforcement de la cybersécurité. Le fait de promouvoir les standards techniques prescrits par l'industrie et reconnus internationalement aide les entreprises à développer et distribuer plus rapidement de nouveaux produits plus sûrs.

Malgré tout, certains États établissent des normes spécifiques à leur pays avec l'argument que cette obligation supplémentaire va dans le sens du renforcement de la cybersécurité. Mais c'est l'effet inverse qui se produit. Les standards imposés par l'Etat, plutôt que de renforcer la sécurité, gèlent l'innovation et obligent les consommateurs et les entreprises à utiliser des produits qui ne satisfont pas totalement leurs besoins.

Éviter les règles de localisation des données

Avec l'avènement des services de Cloud Computing, les entreprises de toute taille partout dans le monde ont désormais accès à des ressources réservées jusque-là aux plus grandes sociétés. Le modèle du Cloud s'appuie pourtant sur des réseaux qui permettent le stockage et le traitement des données dans différents lieux et même dans plusieurs pays. En autorisant la libre circulation des données sur de multiples marchés, les fournisseurs Cloud peuvent apporter de multiples avantages à leurs clients, fiabilité, résilience et services de support 24/24h, par exemple.

En prônant à tort l'hypothèse que les données sont plus en sécurité dans un lieu spécifique, certains pays imposent des règles qui empêchent ou compliquent considérablement les transferts de données entre frontières. Les politiques qui restreignent inutilement la libre circulation des données portent préjudice aux avantages caractéristiques du cloud computing en augmentant les coûts et en menaçant d'interdire l'accès aux nouveaux services Cloud.

Éviter de donner la préférence aux technologies nationales

Des produits et services de pointe sont développés grâce à la collaboration des centres de recherche et de design de pays différents. Les pays devraient donc créer des incitations à la collaboration transfrontalière pour faciliter les transferts volontaires de technologie et des cycles courts de développement et de déploiement de meilleurs produits et services.

Mais certains pays adoptent l'approche opposée : en empêchant la concurrence provenant de l'étranger, ils pensent qu'ils protègent leurs propres champions, qu'ils développent une industrie technologique domestique, et qu'ils renforcent la cybersécurité. Par nature, les technologies nationales sont un sous-ensemble de l'innovation mondiale. Le fait d'empêcher l'exercice de la concurrence de l'étranger dégrade la cybersécurité puisqu'on interdit aux sociétés et agences d'acquérir des produits et services du marché international. De surcroît, de telles règles ont un effet pervers sur les sociétés domestiques spécialistes de la technologie qui ne peuvent envisager de collaborer avec des leaders mondiaux et perdent en compétitivité à l'échelle mondiale, ce qui freine aussi l'innovation mondiale.

TABLEAU DE LA MATURITÉ DES POLITIQUES DE CYBERSÉCURITÉ DANS L'UE (2015)

✔ Oui ✖ Non ◑ Partiellement

#	QUESTION	Allemagne	Autriche	Belgique	Bulgarie	Chypre	Croatie	Danemark	Espagne
	BASES LÉGALES								
1.	Existe-t-il une stratégie nationale de cybersécurité ?	✔	✔	✔	✖	✔	✖	✖	✔
2.	En quelle année la stratégie nationale de cybersécurité a-t-elle été adoptée ?	2011	2013	2012	–	2013	–	–	2013
3.	Existe-t-il une stratégie ou un plan de protection d'infrastructures critiques ?	✔	✔	◑	◑	✖	✖	✖	✔
4.	Existe-t-il une législation ou une règle qui oblige à établir un plan écrit de sécurité de l'information ?	✖	✖	✖	✖	✖	✖	◑	✖
5.	Existe-t-il une législation ou une règle qui oblige à dresser un inventaire des « systèmes » et une classification des données ?	✔	✔	✔	✔	◑	✔	✔	✔
6.	Existe-t-il une législation ou une règle qui impose des pratiques ou des obligations de sécurité en fonction du niveau de risque ?	✔	✔	✔	✔	✖	✔	✔	✔
7.	Existe-t-il une législation ou une règle qui préconise (au moins) un audit annuel de cybersécurité ?	En cours	✔	✖	✖	✖	✖	✖	◑
8.	Existe-t-il une législation ou une règle qui oblige à publier un état des lieux des capacités de cybersécurité à la disposition de l'Etat ?	En cours	◑	✖	✖	✖	◑	✖	✖
9.	Existe-t-il une législation ou une règle qui oblige chaque agence à se doter d'un directeur des services informatiques (DSI) ou de la sécurité ?	✖	✖	✖	✖	✖	✖	✖	✖
10.	Existe-t-il une législation ou une règle qui oblige à déclarer les incidents de cybersécurité ?	✔	✖	◑	✖	✔	✖	✖	✖
11.	Existe-t-il dans la législation ou les règles une définition appropriée de la « protection des infrastructures critiques » ?	✔	✔	✔	✔	✖	✖	✔	✔
12.	Les achats de solutions de cybersécurité dans le public et le privé sont-ils encadrés par les systèmes d'accréditation ou de certification internationaux, sans exigences locales spécifiques ?	✔	✔	◑	N/A	N/A	N/A	✔	✔
	ENTITÉS OPÉRATIONNELLES								
1.	Existe-t-il un centre national d'alerte et de réaction aux attaques informatiques, CERT (computer emergency response team) ou CSIRT (computer security incident response team) ?	✔	✔	✔	✔	✖	✔	✔	✔
2.	En quelle année le CERT (computer emergency response team) a-t-il été établi ?	2012	2008	2008	2008	–	2009	2009	2008
3.	Existe-t-il une autorité nationale compétente en charge de la sécurité informatique et des réseaux ?	✔	◑	✔	✔	◑	✔	✔	✔
4.	Existe-t-il une plate-forme de centralisation des rapports et données concernant les incidents et cybersécurité ?	✔	✔	✔	✔	✖	✔	✔	✔
5.	Des exercices nationaux de cybersécurité sont-ils organisés ?	✔	✔	✔	✔	◑	◑	✔	◑
6.	Existe-t-il une structure nationale de gestion des incidents ayant les capacités de répondre aux incidents de cybersécurité ?	✖	✔	✖	◑	✖	✖	◑	✔
	PARTENARIATS PUBLIC-PRIVÉ								
1.	Existe-t-il un partenariat public-privé officiel en faveur de la cybersécurité ?	✔	✔	◑	◑	◑	◑	✖	✔
2.	L'industrie est-elle organisée (conseils de cybersécurité de représentants d'entreprises ou de l'industrie) ?	✔	✔	✔	◑	✖	✖	✔	✔
3.	Y a-t-il de nouveaux partenariats public-privé en cours ou en projet (si oui, de quelle spécialité) ?	✔	✔	–	✖	✖	✖	✖	–
	PLANS DE CYBERSÉCURITÉ SECTORIELS								
1.	Existe-t-il un plan commun aux secteurs public et privé qui traite de la cybersécurité ?	✖	✔	✖	✖	◑	◑	✖	✔
2.	Des priorités de sécurité par secteur ont-elles été définies ?	✖	✖	✖	✖	✖	✖	✖	◑
3.	Des évaluations des risques pour la cybersécurité ont-elles été réalisées par secteur ?	✖	✖	✖	✖	✖	✖	✖	✖
	ÉDUCATION								
1.	Existe-t-il une stratégie d'éducation pour informer et sensibiliser davantage le jeune public aux risques de cybersécurité ?	◑	✔	◑	◑	✖	✖	✖	✔

Estonie	Finlande	France	Grèce	Hongrie	Irlande	Italie	Lettonie	Lituanie	Luxembourg	Malte	Pays-Bas	Pologne	Portugal	République tchèque	Roumanie	Royaume-Uni	Slovaquie	Slovénie	Suède
✔	✔	✔	✖	✔	✖	✔	✔	✔	✔	✖	✔	✔	Draft	✔	✔	✔	✔	✖	✖
2014	2013	2011	–	2013	–	2014	2014	2011	2013	–	2013	2013	–	2011	2013	2011	2008	–	–
✔	✔	✖	✔	◑	✖	✔	✖	◑	✖	◑	✔	✔	✖	✔	✔	✔	✔	✔	✔
✔	◑	✖	◑	✔	✖	✖	✖	✖	✖	◑	◑	✖	✖	✔	✖	◑	◑	✖	✔
✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✖	✔	✖	✔	✔	✔	✖	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔	✔	✖	✖	✖	✖	✖	✔	◑	◑	◑	◑	✖	◑	◑	✖	✖	✖	◑	✖
✔	✔	✖	✖	✔	✖	✔	✖	◑	✖	✖	✔	✖	◑	✔	✖	◑	◑	✖	✖
✖	✖	✔	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔
✔	✖	✖	✖	✖	✖	✖	✔	✔	✖	✔	✖	✔	✖	✔	◑	✖	✖	✔	✖
✔	✔	✖	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔
✔	✔	◑	✔	✔	N/A	✔	◑	◑	◑	N/A	✔	◑	N/A	◑	◑	◑	✖	N/A	✔
✔	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
2008	2014	2008	2009	2013	–	2014	2006	2006	2011	2002	2012	2008	2008	2011	2011	2014	2009	2010	2003
✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔	✔	✔	✔	◑	✔	✔	✔	◑	◑	◑	✔	◑	◑	◑	◑	✔	✔	◑	✔
◑	✖	✖	✖	✔	✖	✔	✔	◑	◑	✖	✔	✔	◑	✔	◑	✔	✖	✖	◑
◑	◑	✖	✖	◑	✖	◑	✖	✖	✖	◑	✔	✖	◑	✖	✖	✔	✖	✖	◑
◑	✔	✖	✖	◑	✔	◑	✖	◑	✖	✖	✔	◑	✖	✖	◑	✔	◑	◑	◑
✖	✖	◑	✖	✖	✖	◑	◑	◑	◑	✖	–	✖	✖	◑	✔	–	✖	✖	✖
✖	◑	✔	✖	◑	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✔	✖	✖	✖
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	◑	✖	✖	✖
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖
✔	✔	✔	✖	✔	◑	✔	✔	✔	✔	✖	✔	✔	✖	✔	✔	✔	✔	✖	✖

UN CADRE APPROPRIÉ FAVORABLE AU PARTAGE D'INFORMATIONS UTILES

Les incidents ou failles de cybersécurité peuvent avoir un impact majeur sur les États, les sociétés du privé et même les individus. La médiatisation de certains cas de violation amène les gouvernements du monde entier à réfléchir aux moyens de mieux prévenir et détecter ces incidents et les gérer le cas échéant.

L'échange et le partage des bonnes informations au bon moment, ainsi que l'effort coordonné des acteurs concernés, sont les meilleures pistes à suivre pour réduire et contrôler les risques et mieux réagir à de tels cyber incidents.

La question centrale porte sur les conditions à réunir pour que les interlocuteurs parviennent à mettre en commun et à s'échanger des informations utiles. Certains pays envisagent les systèmes obligatoires de notification d'incident, mais ce dispositif seul n'apportera pas une réponse suffisante à la question de la sensibilisation collective et de la préparation. Les échanges volontaires d'information basés sur la confiance s'avèrent être le moyen le plus probant pour établir le partage efficace d'information.

Faciliter le partage d'information utile n'est pas facile. Il faut un environnement favorable, des plates-formes d'échange notamment. Voici quelques-uns des fondamentaux d'un tel environnement :

- **Créer un environnement de confiance :** pour qu'ils soient efficaces, le partage d'information et le signalement d'incident doivent être à la fois encadrés et encouragés. Ce n'est qu'ainsi qu'on instaure le climat de confiance nécessaire pour qu'un tel système fonctionne. Il faut des garanties que l'organisation qui partage des informations ne s'expose pas à des responsabilités excessives, à des litiges, des sanctions ou le risque d'une humiliation publique.
- **Établir un haut niveau de confidentialité :** compte tenu de la nature sensible des informations qui sont partagées concernant un incident ou une cyber menace affectant une infrastructure critique, il faut absolument que soient respectées et maintenues la confidentialité et la sécurité des communications entre l'opérateur de l'infrastructure et toute autorité de supervision, dans le contexte des obligations de transparence imposées à l'autorité.

  Dans certains cas, il peut être nécessaire d'informer le public d'un incident. Il faut alors veiller à établir un dialogue en profondeur entre les sociétés victimes de l'infraction et les autorités avant toute révélation publique pour éviter d'élargir le périmètre de l'attaque, de multiplier les effets de l'incident, de générer de la panique ou de provoquer une humiliation publique.
- **Instaurer la réciprocité :** certes le secteur privé possède et exploite la plus grosse partie des infrastructures critiques des États, mais ce ne doit pas être une raison pour considérer la fourniture des données utiles selon un axe unilatéral, du privé vers le public. Au contraire, il doit s'agir d'un échange mutuel d'information, basé sur la confiance et les intérêts communs.
- **Clarifier les obligations et les rendre cohérentes entre les juridictions :** à mesure que les obligations de notification gagnent toujours plus de domaines et de secteurs géographiques, le risque de conflit entre des obligations légales s'accroît. Pour les organisations présentes dans plusieurs secteurs de différents pays, les questions se posent déjà de savoir ce qu'il faut déclarer, quand et à qui dans un souci de conformité. Mais si un système de notification obligatoire devait être mis en place, il faudrait veiller à instaurer et maintenir autant de cohérence que possible entre les différentes obligations de notification, mais aussi entre les préconisations nationales et régionales.

LES PRATIQUES DE CYBERSÉCURITÉ DE CHAQUE ÉTAT MEMBRE DE L'UE

Les synthèses qui suivent donnent un état des lieux de la cybersécurité, au regard des critères détaillés ci-avant. Il y est précisé quels sont les aspects réglementaires et législatifs en vigueur et quelles entités opèrent actuellement dans chaque juridiction. Les fiches détaillées pour chaque Etat membre de l'UE sont disponibles à l'adresse : www.bsa.org/EUcybersecurity.

ALLEMAGNE

L'Allemagne a une stratégie de cybersécurité complète, adoptée en 2011 et qui s'appuie sur un cadre juridique solide régissant la cybersécurité. L'existence d'un bureau fédéral de la sécurité informatique (le BSI), responsable de la gestion de la sécurité informatique et des communications pour l'Etat allemand, démontre que la cybersécurité est bien à l'ordre du jour du gouvernement.

L'Allemagne dispose aussi d'un réseau de CERT : le centre CERT national, CERT-BUND, collabore étroitement avec les centres CERT d'état et non-gouvernementaux.

Le pays veille à entretenir des partenariats public-privé, comme l'Alliance pour la cybersécurité et le partenariat UP KRITIS, et ses règles nationales ainsi que son arsenal juridique témoignent de l'intérêt porté à cette coopération.

AUTRICHE

La stratégie autrichienne de cybersécurité a été adoptée en 2013. Elle s'inscrit dans une initiative de sécurité des TIC du gouvernement autrichien, comme indiqué dans la stratégie National ICT Security Strategy 2012. La stratégie repose sur un vaste plan qui fait correspondre les objectifs de cybersécurité et des champs d'action organisés.

L'Autriche a un centre national CERT d'alerte et de réaction aux attaques informatiques dont le périmètre est large et bien défini. Il existe des partenariats public-privé sur la cybersécurité dans le pays, comme le Centre for Secure Information Technology Austria (A-SIT) et le Kuratorium Sicheres Österreich.

Les cercles ATC (Austrian Trust Circles) proposent des structures formelles pour les échanges d'information sectoriels relatifs aux infrastructures critiques de différents secteurs. Ces plates-formes sont conçues pour faciliter la création de plans de gestion des risques sectoriels. Les Austrian Trust Circles sont un projet de CERT.at de la chancellerie fédérale de la République d'Autriche.

BELGIQUE

Le gouvernement belge a adopté sa stratégie de cybersécurité en 2012. Le cadre juridique de cybersécurité manque de clarté et d'information sur les conditions de mise en oeuvre de la stratégie.

La Belgique n'a pas de centre national CERT.be d'alerte et de réaction aux attaques informatiques, ni de structure suffisamment coordonnée de signalement des incidents. La Belgique a annoncé récemment le lancement d'un nouveau centre de cybersécurité. BeINIS, un organisme d'état qui noue des relations avec les entités privées et semi-privées, soutient activement la création de partenariats public-privé. .

BULGARIE

Le cadre juridique de cybersécurité est limité en Bulgarie et il n'existe pas de stratégie nationale de cybersécurité. Il n'existe pas non plus de partenariats public-privé formalisés, même si un certain nombre d'événements de cybersécurité et des débats universitaires portent sur les questions de cybersécurité et de protection des infrastructures critiques.

Le CERT Bulgarie est l'entité de cybersécurité la plus significative du pays et elle concentre les récents efforts du gouvernement pour renforcer la cybersécurité.

CHYPRE

Chypre a adopté une stratégie nationale de cybersécurité en 2013, qui prévoit de tenir à jour le cadre juridique de la cybersécurité. Chypre œuvre également en faveur de l'établissement d'un centre CERT national, qui devrait être opérationnel en 2015. Le pays s'intéresse également aux approches sectorielles de gestion de la cybersécurité, et privilégie les secteurs de l'énergie et des services financiers.

CROATIE

La Croatie n'a toujours pas mis en oeuvre de stratégie de cybersécurité ni de système pour encadrer les partenariats public-privé.

La Croatie est dotée de deux centres CERT (computer emergency response team). Le centre National CERT, établi en 2009, coordonne les mesures de sécurité et la gestion des incidents pour les utilisateurs d'adresses IP croates ou du domaine .hr. Le CERT ZSIS du bureau de la sécurité des systèmes d'information couvre les institutions du gouvernement croate.

DANEMARK

Le Danemark n'a pas de stratégie nationale de cybersécurité, ni de loi encadrant la question. Le Danemark a récemment adopté une loi qui prévoit le remplacement de l'actuel CERT du gouvernement par le futur Centre pour la cybersécurité, dont le périmètre et les pouvoirs doivent encore être confirmés.

Le secteur privé danois a mis en place un cadre formel de coopération sur les questions de cybersécurité via le Conseil pour la sécurité digitale.

ESPAGNE

L'Espagne a adopté une stratégie nationale de cybersécurité en 2013. C'est un document complet, qui fixe des objectifs et décrit les actions ciblées. Cette stratégie fait référence au Plan national de sécurité et aux lois de sécurité existantes, qui constituent un ensemble juridique

Il existe deux centres CERT en Espagne, INTECO-CERT et CCN-CERT, et un centre national de protection des infrastructures critiques (CNPIC). Ce dernier est la première agence de sécurité de l'information et de cybersécurité, alors que le rôle des centres CERT se limite à la gestion des incidents de cybersécurité. Le CNPIC est chargé de coordonner les activités de coopération entre les secteurs public

et privé. Il organise des groupes de travail par secteur et œuvre pour le développement de plans de cybersécurité sectoriels.

La coopération avec le secteur privé est formalisée par le conseil consultatif national sur la cybersécurité, établi en 2009, dont les membres sont des représentants du secteur privé. Le conseil fait des propositions de règles au gouvernement, mais son statut n'est pas très clair. Les associations du secteur privé sont actives également, avec deux organes prépondérants qui se consacrent spécifiquement à la cybersécurité et à la sécurité de l'information.

ESTONIE

L'Estonie est l'un des premiers pays à avoir développé une stratégie nationale de cybersécurité en 2008, qu'ils ont actualisée en 2014. Le pays dispose également d'un large arsenal législatif qui couvre la sécurité de l'information et la cybersécurité. L'Estonie a mis en place un CERT, CERT Estonie, sous le contrôle de l'Autorité des systèmes informatiques. Il faut aussi noter que le Centre d'excellence de la cybersécurité de l'OTAN est basé en Estonie.

S'il n'existe pas de partenariat public-privé formalisé, des entités du public collaborent dans les faits avec des organisations du privé.

FINLANDE

La Finlande a publié une stratégie complète de cybersécurité. A celle-ci s'ajoute un cadre juridique solide portant sur un certain nombre d'aspects importants pour la cybersécurité. L'autorité nationale de la cybersécurité en Finlande est en phase de transition, avec la fusion de deux CERT d'état et la création d'un Centre de la cyber sécurité.

FRANCE

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. 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.

GRÈCE

La Grèce n'a pas de véritable stratégie de cybersécurité ni de législation dédiée à la cybersécurité. Le cadre juridique et institutionnel en faveur de la cybersécurité est aussi limité. Le centre national d'alerte et de réaction aux attaques informatiques, NCERT-GR, se limite aux institutions d'Etat et aux exploitants de l'infrastructure critique.

Il n'existe pas vraiment de partenariat public-privé en Grèce et le gouvernement ne soutient pas activement leur création, ni les efforts de coopération avec le secteur privé.

HONGRIE

La stratégie nationale de cybersécurité a été adoptée en 2013. Elle couvre les principes clés de cybersécurité, fait l'état des lieux de la cybersécurité en Hongrie et pose les objectifs à atteindre à l'avenir. L'arsenal législatif dédié à la cybersécurité est limité en Hongrie.

Plusieurs autorités publiques jouent un rôle dans la cybersécurité, et notamment l'Autorité nationale de sécurité qui se charge de la sécurité de l'information, et le Centre de cybersécurité, qui dépend des services de renseignement et qui traite exclusivement de la cybersécurité. Le CERT-Hongrie, centre national d'alerte et de réaction aux attaques informatiques, est limité aux institutions gouvernementales. Et alors que le centre national de cybersécurité a pour mission de traiter avec le secteur privé, il n'existe pas de partenariats public-privé formalisés.

IRLANDE

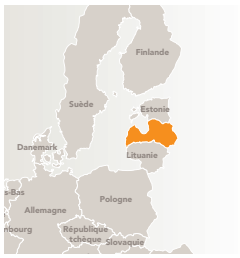
Le cadre juridique et réglementaire d'Irlande est très limité pour ce qui concerne la cybersécurité. Une stratégie de cybersécurité est en cours d'élaboration mais il n'existe pas de calendrier de publication, ni d'adoption. L'Irlande est aussi l'un des rares pays de l'Union européenne sans centre CERT opérationnel pour le moment, mais des efforts sont en cours en ce sens.

S'il n'existe pas de partenariat public-privé formalisé pour la cybersécurité, les entités du secteur privé, dont Infosecurity Ireland, semblent être relativement actives dans ce domaine. L'Irlande a aussi organisé un certain nombre de campagnes d'information sur la cybersécurité, comme « Make IT Secure », dont une campagne télévisée de promotion des ressources en ligne.

ITALIE

L'Italie a actualisé ses lois de sécurité en 2007 et fait adopter des plans de cybersécurité en 2013 et 2014, si bien que le cadre juridique régissant la cybersécurité est solide. La stratégie italienne de cybersécurité préconise la voie des partenariats public-privé, mais il n'existe pas de coopération formalisée pour le moment.

Le centre CERT-PA a été créé en 2014. Il est responsable des systèmes d'alerte de cybersécurité et de la coordination des mesures de gestion des incidents pour les institutions de l'Etat.



LETTONIE

La Lettonie a publié en 2014 une stratégie de cybersécurité qui stipule des objectifs clairs et les dates de mise en œuvre correspondantes. Le pays dispose également d'un arsenal juridique solide en faveur de la cybersécurité, dont un pilier important est la loi de sécurité des technologies de l'information adoptée en 2010. Cette loi spécifie les rôles et responsabilités du centre national d'alerte et de réaction aux attaques informatiques, le CERT.LV.

La stratégie de cybersécurité encadre les conditions d'établissement de partenariats public-privé formalisés, mais aucune plate-forme n'existe pour le moment.

LITUANIE

La Lituanie a publié une stratégie de cybersécurité en 2011, mais il existe peu d'information quant à sa mise en œuvre. Le centre lithuanien d'alerte et de réaction aux attaques informatiques, le CERT-LT, englobe l'ensemble des réseaux nationaux, et non les seuls réseaux d'état, et le Conseil d'état de gestion des ressources de l'information est un organe puissant d'élaboration et de gestion des règles.

La stratégie de cybersécurité reconnaît la valeur et la nécessité des partenariats public-privé mais il n'existe pas de coopération formalisée ni systématique.

LUXEMBOURG

Le Luxembourg a une stratégie de cybersécurité relativement limitée, publiée en 2013, qui contient certains principes clés d'orientation mais propose peu d'information sur leur mise en œuvre. Le cadre légal en faveur de la cybersécurité doit encore être développé. La stratégie de cybersécurité reconnaît comme principe phare la nécessité d'encourager la coopération public-privé, mais aucune coopération formelle n'est connue.

Il existe deux centres CERT au Luxembourg : le CIRCL est un organe de coordination des réponses qui couvre l'ensemble des organisations présentes au Luxembourg, tandis que le GOVCERT.LU se concentre sur les seules autorités du public. Enfin, l'agence gouvernementale CASES de sécurité de l'information s'occupe d'activités de sensibilisation et de la promotion des meilleures pratiques.

MALTE

Malte doit encore développer un cadre juridique et réglementaire suffisamment complet pour régir la cybersécurité, même si la stratégie Digital Malta et le plan de e-gouvernement promettent l'élaboration d'une stratégie de cybersécurité.

L'agence MITA (Malta Information Technology Agency) semble être active dans le domaine de la cybersécurité. Le centre CERT national, CSIRT Malte, coordonne les mesures de gestion des incidents pour les entités en lien avec l'infrastructure critique de Malte.

PAYS-BAS

Le cadre juridique et réglementaire des Pays-Bas concernant la cybersécurité est bien développé et mature ; il inclut la stratégie nationale de cybersécurité 2, adoptée en 2013, seconde stratégie en date puisque le cadre de cybersécurité du pays est renouvelé tous les deux ans.

Les Pays-Bas ont aussi un centre national de cybersécurité CERT, au périmètre élargi, qui a vocation à centraliser toutes les pratiques et procédures liées à la cybersécurité. Ce centre participe aussi activement aux efforts des centres ISAC (Information Sharing and Analysis Centres) de partage et d'analyse de l'information pour les secteurs concernés par les infrastructures critiques.

POLOGNE

La Pologne a une stratégie de cybersécurité complète aux objectifs clairement définis. Comme elle a été adoptée en 2013, la plupart de ses recommandations sont toujours en cours de mise en oeuvre. Le cadre juridique de cybersécurité est incomplet et doit encore être développé.

Plusieurs centres CERT existent en Pologne, dont CERT.GOV.PL, qui régit les entités d'Etat et celles liées aux infrastructures critiques, et qui agit en qualité d'autorité de cybersécurité également. CERT Pologne est un centre CERT universitaire, qui couvre tout le réseau .pl avec un mandat semi-officiel.

PORTUGAL

Il reste encore au Portugal à développer un cadre juridique et réglementaire suffisamment complet pour régir la cybersécurité et à élaborer sa stratégie de cybersécurité. Aucune coopération public-privé n'est formalisée pour encore.

Le pays a un centre national CERT, le CERT-PT, et un centre national de cybersécurité. Ce dernier a été établi par l'Autorité nationale de sécurité et a pour mission de coopérer avec le secteur privé en cas d'incident de cybersécurité.

RÉPUBLIQUE TCHÈQUE

La stratégie de cybersécurité de la République tchèque pour la période 2011-2015 a été publiée en 2011. Elle établit des principes de cybersécurité de portée générale et des objectifs clairs. Le 1er janvier 2015, l'Act on Cyber Security a été ratifié : il s'agit d'une loi qui régit les principaux aspects de la cybersécurité, complétés par plusieurs réglementations importantes.

Le pays a aussi créé un centre CERT national, CSIRT.CZ, et un CERT dédié aux agences gouvernementales : GOVCERT.CZ.

Le centre national de cybersécurité a été créé le 1er janvier 2015 pour promouvoir les partenariats public-privé. De plus, la République tchèque procède à une évaluation des risques de sécurité par secteur en coopération avec les secteurs universitaire et privé. Le projet est le premier à porter sur l'évaluation de la cybersécurité.

ROUMANIE

La stratégie de cybersécurité adoptée par la Roumanie en 2013 est vague. Son cadre juridique est limité, même si des propositions de lois ont été soumises au parlement en vue de leur adoption. Le centre national d'alerte et de réaction aux attaques informatiques, CERT-RO, couvre tous les utilisateurs des réseaux roumains. La stratégie de cybersécurité préconise l'établissement de deux nouvelles agences de cybersécurité.

ROYAUME-UNI

Le Royaume-Uni dispose depuis 2011 d'une stratégie de cybersécurité complète, qui est assortie d'un cadre juridique de cybersécurité solide et est soutenue par deux CERT : CERT-UK est à la disposition des exploitants des infrastructures critiques tandis que GovCertUK soutient les agences gouvernementales. Le conseil national de sécurité et l'Office of Cyber Security and Information Assurance figurent parmi les autres organes officiels du pays.

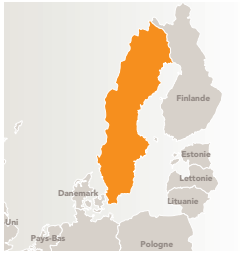
Le Royaume-Uni dispose aussi d'un système de partenariats public-privé bien développé avec une forte participation active du privé. Cette approche collaborative s'appuie sur la stratégie de cybersécurité en place. Le Centre for the Protection of National Infrastructure (CPNI), par exemple, organise des échanges d'information par secteur et couvre 14 secteurs.

SLOVAQUIE

La Slovaquie a adopté en 2009 sa première stratégie de cybersécurité sur 5 ans. Les détails relatifs à la prochaine stratégie 2014-2020 restent limités. Le centre CERT de Slovaquie, CSIRT.SK, régit les agences d'état et les exploitants des infrastructures critiques,. Il n'existe pas de partenariat public-privé formalisé en faveur de la cybersécurité.

SLOVÉNIE

Il reste encore à la Slovénie à développer un cadre juridique et réglementaire suffisamment complet pour régir la cybersécurité. Le pays doit encore adopter une stratégie nationale de cybersécurité. Le centre national SI-CERT supervise tous les réseaux opérationnels en Slovénie. Il n'existe pas de partenariat public-privé formalisé en faveur de la cybersécurité.



SUÈDE

La Suède n'a pas de stratégie nationale de cybersécurité pour le moment, mais des efforts de développement sont en cours. Il n'existe pas de lois régissant spécifiquement la cybersécurité en Suède.

La Suède a par contre un centre CERT, CERT-SE, dont le périmètre couvre tous les réseaux suédois. Mais l'agence MSB des contingences civiles suédoises est l'autorité nationale en charge de la sécurité d'information et a beaucoup œuvré pour asseoir la réputation de cybersécurité du pays. MSG est l'entité de centralisation des aspects de sécurité de l'information avec une forte présence publique.

À PROPOS DE LA BSA

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.

À PROPOS DE GALEXIA

Galexia (www.galexia.com) est à la pointe de la recherche internationale et du conseil dans les domaines de la vie privée, de l'identité, de la cybersécurité et du cloud, avec un focus particulier sur les problématiques de droit et de régulation mondiales et transfrontalières. Nous avons l'expertise des complexités politiques qui se présentent aux pays faisant face à des problèmes de cybersécurité. Nous prodiguons du conseil sur les stratégies nationales de cybersécurité, sur la protection des infrastructures vitales et sur la mise en place de systèmes d'alerte et de gestion de la cybersécurité.

Nous travaillons étroitement avec différentes catégories de clients internationaux, privés ou publics, afin de produire des résultats clairs et efficaces provenant d'une recherche basée sur des éléments concrets. Nous utilisons des outils de reporting collaboratifs basés sur le cloud afin de fournir un accès en temps réel à nos recherches et à nos analyses.

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom

T: +44.207.340.6080
F: +44.207.340.6090