Pratiques en matière d'assurance de la cybersécurité

Période d'études

2022-2025

Question 3/2

Sécurisation des réseaux d'information et de communication: Bonnes pratiques pour créer une culture de la cybersécurité

Produit intérimaire 2023

Résumé analytique

La Conférence mondiale de développement des télécommunications, tenue à Kigali en 2022, a examiné le mandat de la Question 3/2, qui porte sur l'échange de données d'expérience sur les pratiques en matière de cybersécurité. Les menaces à la cybersécurité sont une préoccupation majeure à l'échelle mondiale, la dépendance croissante à l'égard de la technologie entraînant une escalade des risques et des conséquences des cyberattaques. Les pratiques en matière d'assurance de la cybersécurité sont apparues comme un élément essentiel de la protection des réseaux, des systèmes et des données contre les activités malveillantes.

Le présent rapport rend compte des contributions et des discussions des réunions sur la Question 3/2 et d'un atelier consacré aux pratiques en matière d'assurance de la cybersécurité. Les six principaux points à retenir de ces discussions sont présentés ci-dessous:

1. Différents niveaux critiques et niveaux de risques nécessitent différents niveaux d'assurance. Les évaluations des risques peuvent aider à déterminer le niveau d'assurance approprié, compte tenu de la sensibilité des données et des actifs protégés, des conséquences d'une violation ainsi que de l'environnement des menaces.
2. L'engagement avec les organisations partenaires, l'industrie et les multiples parties prenantes peut être un moyen efficace de renforcer l'assurance de la cybersécurité. La coopération entre les décideurs, les organisations de la société civile et le secteur privé peut stimuler la demande de sécurité et éclairer l'élaboration de politiques et de réglementations.
3. Envisager une approche réglementaire évolutive, éclairée par le dialogue et les consultations. Les pratiques en matière d'assurance de la cybersécurité peuvent être mises en place à titre volontaire avant de devenir obligatoires, en fonction de la nécessité de mesures plus strictes pour se prémunir contre les cyberattaques.
4. Compte tenu du paysage dynamique des menaces et de l'évolution des risques de cybersécurité, les pratiques en matière d'assurance de la cybersécurité devraient être revues et adaptées au fil du temps. Des audits internes réguliers et l'abonnement à des renseignements sur les menaces sont considérés comme de bonnes pratiques.
5. Des efforts sont faits pour sensibiliser les consommateurs et les fabricants à l'importance de la cybersécurité et aux avantages de choisir des produits plus sûrs. Les systèmes d'étiquetage et les campagnes de sensibilisation à la cybersécurité peuvent aider à informer les utilisateurs sur la sécurité des produits technologiques.
6. Les accords de réciprocité peuvent contribuer à faciliter la conformité pour les acteurs industriels opérant sur de multiples marchés, tandis que l'harmonisation des exigences de sécurité de base réduit le fardeau réglementaire pesant sur les fournisseurs de produits et de services.

Introduction

Au cours de la dernière Conférence mondiale de développement des télécommunications, tenue à Kigali (Rwanda) en juin 2022, le mandat de la Question 3/2 "Sécurisation des réseaux d'information et de communication: Bonnes pratiques pour créer une culture de la cybersécurité" a été examiné et l'un des thèmes à étudier était "Partager des données d'expérience sur les pratiques en matière d'assurance de la cybersécurité".[1]

Le champ d'application approuvé pour la Question 3/2 reconnaît que les menaces à la cybersécurité continuent d'être une préoccupation majeure pour les gouvernements, les organisations et les particuliers dans le monde entier. Avec le recours croissant à la technologie, les risques potentiels et les conséquences des cyberattaques augmentent également et les cyberattaques deviennent de plus en plus rentables[2]. Les cybercriminels exercent une activité lucrative dont le coût est estimé à 8 000 milliards USD dans le monde[3].

Les pratiques en matière d'assurance de la cybersécurité[4] sont apparues comme un élément essentiel de la protection des réseaux, des systèmes et des données contre les activités malveillantes. Celles-ci désignent en gros les procédures utilisées pour s'assurer que des contrôles appropriés sont en place pour protéger la confidentialité, l'intégrité et la disponibilité des dispositifs, systèmes, réseaux et données électroniques. Bien qu'ils n'empêchent pas directement les cyberattaques, leur objectif, s'il est correctement mis en œuvre, est de minimiser le risque que de telles attaques se produisent. Les pratiques en matière d'assurance de la cybersécurité peuvent être vérifiées par rapport à des contrôles, directives et normes de sécurité spécifiques et peuvent être imposées par la réglementation ou adoptées volontairement par l'industrie. Cependant, il n'existe pas d'approche universelle, les autorités nationales et les régulateurs sectoriels utilisant souvent des pratiques différentes, allant de l'auto-évaluation et des lignes directrices volontaires aux systèmes d'étiquetage et aux contrôles de conformité rigides.

Bien qu'il n'y ait pas d'approche unique à recommander, on observe, depuis ces dernières années et ces derniers mois, une tendance durable privilégiant l'adoption de pratiques d'assurance de la cybersécurité partout dans le monde, avec des évolutions différentes dans plusieurs pays et régions. À titre d'exemple de cet élan, l'Organisation de coopération et de développement économiques a lancé, en décembre 2022, la Recommandation du Conseil sur la sécurité numérique des produits et services, qui préconise l'adoption de politiques visant à améliorer la sécurité numérique des produits et services qui sont proportionnés au risque, en commençant par une approche souple fondée sur des mesures politiques volontaires, et étudier la nécessité de mesures obligatoires[5].

Le présent rapport rend compte des contributions et des discussions des réunions sur la Question 3/2 et de l'atelier consacré aux pratiques en matière de garantie de la cybersécurité. L'atelier public d'une journée, tenu à Genève le 23 mai 2023, a été l'occasion d'explorer le paysage mondial de l'assurance en matière de cybersécurité dans divers domaines (Internet des objets (IoT), télécommunications, etc.) en présentant un éventail de pratiques et de points de vue dans le monde entier. Elle a rassemblé des États Membres, des représentants de l'industrie, des autorités techniques ainsi que des représentants de la société civile.

L'équipe de direction pour la Question 3/2 souhaite saisir cette occasion pour remercier tous les orateurs et les auteurs de contributions pour leurs précieuses contributions sur ce sujet. Cette entreprise ne serait pas possible sans leur engagement.

À la lumière des précieuses contributions reçues, le présent rapport présente principalement les défis rencontrés, les répercussions et les enseignements tirés à ce jour de l'examen et de la mise en œuvre des pratiques en matière d'assurance de la cybersécurité, à travers la présentation de six points à tirer.

Ces enseignements peuvent être une contribution importante pour les membres de l'UIT afin d'évaluer les pratiques existantes et de déterminer s'il est nécessaire d'adopter des approches nouvelles ou différentes, compte tenu de l'expérience acquise et des enseignements tirés par d'autres administrations et organisations.

Premier point à retenir: Différents niveaux critiques et niveaux de risques nécessitent différents niveaux d'assurance

Lorsqu'on envisage de mettre en œuvre des pratiques d'assurance en matière de cybersécurité, il est essentiel de déterminer d'abord ce qu'une entité essaie de protéger et les risques auxquels sont exposés les actifs identifiés. Les pays et les entreprises qui souhaitent se prémunir contre les cyberattaques devraient identifier en priorité les systèmes et les biens qui ont besoin d'être protégés et évaluer leurs vulnérabilités. À cet égard, un plan directeur pour la réalisation d'évaluations des risques est un outil utile. L'un des cadres les plus connus est le cadre de cybersécurité du National Institute for Standards and Technnology (NIST)[6], qui est en cours de mise à jour[7] et contient une approche largement utilisée pour aider à déterminer et à minimiser les risques organisationnels. Il établit des lignes directrices non réglementaires permettant aux organisations du monde entier d'identifier leur propre environnement de risque et d'appliquer des contrôles de cybersécurité appropriés à cet égard. Le cadre révisé, dont la version finale doit être établie d'ici à

1 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/ToR/Q3-2.aspx#Question
2 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090023PDFE.pdf
3 https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023
4 La sécurité opérationnelle est étroitement liée aux pratiques en matière d'assurance de la cybersécurité, en ce sens que la sécurité opérationnelle peut fournir une base solide pour les pratiques en matière d'assurance. Broadcom, Vice-Président de la CE 17 de l'UIT-T, a présenté le modèle de bonnes conditions en soulignant qu'il se compose de quatre éléments clés, à savoir les personnes et les processus, les connaissances, les produits de sécurité (sécurité exogène) et la sécurité des actifs (sécurité endogène). Voir "Réduire les risques et protéger la réputation", https://www.itu.int/md/T22-SG17-C-0214/en.
5 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481
6 https://www.nist.gov/cyberframework
7 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

début 2024, s'appuie sur un engagement large et à long terme avec la communauté des parties prenantes qui utilisent ces lignes directrices, ainsi que sur un alignement continu sur d'autres normes internationales.

Lors de l'atelier, le représentant du NIST a souligné que la position bénéfique de l'organisation en tant qu'organisme non réglementaire a permis un engagement plus profond avec les parties prenantes de l'industrie du monde entier pour comprendre les défis réels et recevoir des commentaires, qui ont été intégrés aux nouvelles lignes directrices[8]. Conçus pour être adaptables et flexibles, ils s'appliquent à toutes les organisations et à tous les secteurs. BitSight, Membre du Secteur de l'UIT-D, a parlé de sa plate-forme, qui intègre le cadre de cybersécurité du NIST et qui a été utilisée par divers organismes publics responsables de la cybersécurité (équipes d'intervention en cas d'urgence informatique (CERT), agences nationales de cybersécurité, régulateurs des télécommunications, etc.)[9]. Grâce à la plate-forme, les pays peuvent évaluer les risques de leurs infrastructures et actifs considérés comme étant essentiels et mesurer leurs facteurs de risque.

Les évaluations des risques peuvent également aider à déterminer quel niveau de garantie est approprié compte tenu de la sensibilité des données et des actifs protégés, des conséquences qu'aurait une atteinte ainsi que de l'environnement de la menace (c'est-à-dire si une entité est susceptible de subir une cyberattaque). Dans certains cas, les niveaux de garantie seront dictés par des exigences réglementaires. Plus le niveau de garantie est élevé, plus les contrôles de sécurité sont stricts. Par exemple, un faible niveau de garantie pourrait nécessiter un mot de passe système ou un pare-feu, tandis qu'un niveau de garantie plus élevé nécessiterait l'ajout de contrôles plus avancés tels que le cryptage avancé et l'authentification à plusieurs facteurs.

Bien que les pratiques d'assurance en matière de cybersécurité augmentent les budgets des technologies de l'information, ne pas mettre en place de contrôles de sécurité peut être plus coûteux. Au cours de l'atelier, les représentants ont exhorté l'auditoire à réfléchir aux coûts de subir une cyberattaque non seulement en termes financiers: le coût supplémentaire de réputation peut être beaucoup plus dommageable. Perdre la confiance des clients et des citoyens a un effet à long terme qui va au-delà du coût financier et les organisations doivent être en mesure de le comprendre stratégiquement. De même, pour le secteur public, les attaques réussies peuvent avoir une incidence sur la fourniture de services publics et sur des activités critiques, dont la perturbation ne peut pas être évaluée uniquement en termes financiers, car elle affecte la vie des citoyens.

Deuxième point à retenir: S'engager avec des organisations partenaires, l'industrie et de multiples parties prenantes peut être un moyen efficace de renforcer l'assurance de la cybersécurité

Premièrement, il est important de comparer les initiatives à d'autres, de comprendre les meilleures pratiques et d'apprendre des succès et des erreurs des autres lors de l'élaboration des initiatives. Deuxièmement, il est important de s'engager avec de multiples parties prenantes, y compris l'industrie, afin d'obtenir des informations importantes pour l'initiative elle-même dans le cadre de cette élaboration.

Alors que les pratiques en matière d'assurance de la cybersécurité deviennent de plus en plus nécessaires, elles peuvent être encore difficiles à appliquer dans les pays les moins avancés. Le représentant de Cyber Defense Africa (CDA) au Togo a expliqué les difficultés rencontrées sur le marché local pour fournir une garantie de cybersécurité aux opérateurs de services essentiels (ESO)[10]. Le manque de financement, le manque de confiance dans le gouvernement en tant que fournisseur de services et le manque de capacités humaines et d'installations locales ont été cités au nombre des problèmes rencontrés. Pour aider les ESO à se conformer aux contrôles de cybersécurité récemment publiés, le Gouvernement du Togo a créé un partenariat public-privé avec un grand fournisseur de cybersécurité réputé pour fournir des services de cybersécurité dans les secteurs public et privé. Grâce à ce modèle, le Togo a créé la CDA en tant que fournisseur local de cybersécurité autosuffisant et de haute qualité pour soutenir les ESO sur une base non obligatoire. Le modèle d'autosuffisance employé a permis au Togo de relever les nombreux défis mentionnés ci-dessus et de commencer à encourager les talents locaux dans le domaine de la cybersécurité, ainsi qu'à favoriser le développement du marché local. Le représentant a souligné l'importance de la CDA en tant qu'entité privée sur un marché concurrentiel afin de garantir l'adaptabilité, la haute qualité des services et des prix compétitifs.

Il est également important d'encourager la coopération entre les décideurs qui peuvent définir l'environnement réglementaire et les organisations de la société civile qui peuvent stimuler la demande de sécurité et éclairer l'élaboration de politiques et de réglementations sur la base des pratiques régionales et internationales existantes et recensées. Par exemple, DiploFoundation est une organisation internationale proposant des programmes de formation, de renforcement des capacités aux gouvernements, aux régulateurs, aux entreprises, à la société civile sur les questions d'actualité liées à la cybersécurité, et impliquée dans le Dialogue de Genève sur les comportements responsables dans le cyberespace[11]. En 2020, le Dialogue de Genève a produit un ensemble de bonnes pratiques[12] qui comprend des définitions suggérées de la conception sécurisée et de la gestion des vulnérabilités, des bonnes pratiques industrielles, de la modélisation des menaces, de la

[8] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090017PDFE
[9] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090024PDFE
[10] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090025PDFE
[11] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090020PDFE
[12] https://genevadialogue.ch/goodpractices/

sécurité des tiers et de la chaîne d'approvisionnement, du développement sécurisé, de la gestion des vulnérabilités et de la divulgation, ainsi que de la culture organisationnelle. Le Forum mondial sur la cyberexpertise (GFCE) est une plate-forme internationale qui soutient la coordination des projets, encourage le partage des connaissances et des compétences, fait correspondre les demandes aux offres de soutien au renforcement des capacités et développe des projets de recherche[13]. Le GFCE a créé quatre pôles régionaux – dans les îles du Pacifique, en Afrique, dans la région Amériques et dans les Caraïbes et en Asie du Sud-Est. Compte tenu de sa présence mondiale et de l'appui varié qu'il propose dans les pays en développement, il est bien placé pour faire connaître des points de vue plus divers sur les besoins et les exigences en matière de renforcement des cybercapacités. Le GFCE dispose d'un portail en ligne qui sert de répertoire des projets en cours et mis en œuvre dans le domaine du renforcement des cybercapacités, à l'échelle mondiale, ainsi que des ressources et des outils. Un tel portail contribue également à réduire tout chevauchement d'activité et à identifier certains programmes ou certaines lacunes et modèles dans l'offre de renforcement des capacités.

Troisième point à retenir: Envisager une approche réglementaire en évolution, qui s'appuie sur le dialogue et les consultations

Dans de nombreux cas, les pratiques en matière d'assurance de la cybersécurité seront mises en place sur une base volontaire avant de devenir obligatoires. Le changement se produit généralement lorsque les gouvernements considèrent que l'industrie n'en fait pas assez pour sécuriser les produits et que les consommateurs n'ont pas nécessairement les connaissances nécessaires pour évaluer si les produits sont sûrs ou non. Cela peut conduire les gouvernements et les autorités nationales à agir et à stipuler des pratiques en matière d'assurance qu'ils attendent de l'industrie. Par exemple, au Brésil, le régulateur des télécommunications, Anatel, a créé un système d'organismes de certification et de laboratoires de test dans le pays pour la certification des équipements de locaux d'abonné (CPE, ou passerelles domestiques). L'approche d'Anatel a toujours consisté à fournir des lignes directrices volontaires en matière de cybersécurité pour le secteur des télécommunications. Toutefois, en procédant à des évaluations des risques, elle a constaté que les recommandations n'étaient pas suffisantes pour les équipements d'abonné, compte tenu des vulnérabilités et des menaces associées à ce type d'équipement, et qu'il était nécessaire d'établir des exigences minimales de sécurité obligatoires pour ces produits. Ces exigences obligatoires pour les fournisseurs de services de communication (CSP) ont été publiées début 2023 et se concentrent sur des vulnérabilités telles que des mots de passe non sécurisés et des composants de rechange inutilement activés. Les exigences entreront en vigueur au début de 2024 dans le cadre des tests de laboratoire obligatoires pour l'approbation des produits[14]. Anatel a expliqué que le passage d'une approche non obligatoire à une exigence de certification obligatoire de cybersécurité pour un ensemble spécifique d'équipements n'était possible qu'après un débat approfondi avec le secteur.

De même, l'Agence nationale de cybersécurité (NCA) du Royaume d'Arabie saoudite a présenté son initiative visant à créer un écosystème indépendant de vérification et de validation (IV&V)[15] destiné à tester et certifier les produits dans une perspective de garantie de la cybersécurité à l'échelle nationale du pays. Cette initiative vise en outre à identifier et à classer les matériels et les logiciels très sensibles aux cyberrisques et aux cybermenaces. De plus, elle cherche à contribuer au développement des capacités humaines dans le système IV&V. Sa feuille de route envisage de commencer par un programme volontaire avant d'en faire une obligation impérieuse. L'autorité a aussi mentionné l'importance pour un tel écosystème de devenir "autosuffisant", ce qui a orienté l'approche de la NCA visant à inciter les acteurs du marché à mener ce type d'évaluation.

Dans le domaine de la sécurité de l'Internet de objets (IoT), le Royaume-Uni a également présenté une étude de cas sur l'évolution d'une approche volontaire vers une approche obligatoire. Ces dernières années, le Royaume-Uni a décidé d'imposer, par voie législative, une exigence de sécurité de base pour les produits grand public IoT, sur la base de la norme ETSI 303 645, première norme de cybersécurité applicable à l'échelle mondiale pour les dispositifs IoT grand public. Au Royaume-Uni, les fabricants, importateurs et distributeurs devront se conformer à trois des 13 lignes directrices de l'ETSI en matière de sécurité, et la loi donne au gouvernement le pouvoir d'adopter des exigences supplémentaires si nécessaire, en fonction des évaluations régulières des menaces. La décision d'imposer des exigences de sécurité de base a suivi une période d'adoption volontaire. En 2018, le pays a formulé un code de pratique volontaire[16] pour la sécurité IoT grand public, mais la conformité de l'industrie n'était pas comme prévu. Les données recueillies dans le cadre d'exercices de consultation ont montré que les consommateurs apprécient la sécurité et sont prêts à payer un prix plus élevé pour des produits sûrs. Cependant, les menaces de sécurité ne sont pas soumises au même niveau de réglementation stricte que la sécurité des produits, ce qui entraîne un manque de transparence de la part des fabricants et une adoption plus lente des politiques de sécurité. Les éléments recueillis ont également révélé que le marché des produits connectables pour le consommateur décourage l'adoption de fonctionnalités de sécurité de base, puisque les consommateurs supposent massivement que les produits sont déjà sécurisés. Le régime vise à combler cette lacune en rendant obligatoires des éléments du code de bonnes pratiques pour s'assurer que les fabricants sont conscients des vulnérabilités et prennent des mesures pour les atténuer. Le régime PSTI (Sécurité du produit et infrastructure des télécommunications) entrera en vigueur en avril 2024 et s'appliquera à tout produit grand public pouvant se connecter à Internet[17].

[13] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090021PDFE
[14] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090018PDFE
[15] https://nca.gov.sa/en/news?item=535
[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
[17] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090014PDFE

L'un des défis identifiés est l'impact possible sur les petites et micro-entreprises qui pourraient avoir des difficultés à se conformer au nouveau régime. L'autorité d'application du Royaume-Uni élabore des lignes directrices pour atténuer toute incidence disproportionnée. En plus de la collaboration avec l'industrie, le Royaume-Uni a indiqué que les trois principales exigences à imposer dans le cadre du régime ont été identifiées et communiquées de manière transparente depuis plusieurs années. Au fil des ans, le Royaume-Uni a mené des exercices sur le processus de mise en œuvre du régime, y compris les exigences en matière de mots de passe, l'architecture fondamentale du produit, l'exposition aux vulnérabilités et les exigences de transparence de la sécurité. L'analyse d'impact a montré que, globalement, les avantages de la réduction du volume des cyberattaques contre les consommateurs et les entreprises devraient dépasser les coûts associés au régime. Comme la loi PSTI 2022 est la première législation obligatoire sur les produits de cybersécurité au monde, le coût de l'application du régime est incertain, mais les premières estimations suggèrent que le financement alloué sera suffisant.

Dans certains cas, la distinction entre le fait qu'une pratique d'assurance a été mandatée ou maintenue volontaire est dictée par qui est l'utilisateur ou le client. Par exemple, la République de Corée a lancé son programme de garantie de la sécurité dans le nuage (CSAP), certification de sécurité pour les services d'informatique en nuage[18]. En général, la certification CSAP relève d'une base volontaire. Toutefois, les clients du secteur public (c'est-à-dire les organismes publics) sont tenus d'utiliser un service en nuage qui a obtenu la certification CSAP conformément à la réglementation pertinente, de sorte que les fournisseurs de services en nuage doivent obtenir une certification lorsqu'ils fournissent de tels services à des organismes publics.

Quatrième point à retenir: Compte tenu du paysage dynamique des menaces et de l'évolution des risques en matière de cybersécurité, les pratiques d'assurance en la matière ne peuvent pas être statiques et devraient être revues et adaptées au fil du temps

La réalisation régulière d'audits internes qui peuvent aider à cerner les lacunes dans les contrôles et les risques d'exposition, ainsi que l'abonnement aux renseignements sur les menaces, sont considérés comme de bonnes pratiques. Même si un produit est certifié, il pourrait, au cours de son cycle de vie, souffrir de failles de sécurité. Un processus de certification nécessite la soumission d'informations à un moment précis, ce qui ne tient pas compte des changements dynamiques des menaces à venir. Une étude récente de BitSight a montré une forte corrélation entre la faible "cadence de correction des correctifs" pour les vulnérabilités et la probabilité de subir un incident de cybersécurité[19], soulignant l'importance de la mise à jour des systèmes dès que des correctifs de sécurité sont disponibles, compte tenu de la répartition différente des correctifs signalés à travers le monde.

Les tests de pénétration, ou "tests d'intrusion", sont des exercices d'assurance de la sécurité qui aident à évaluer la sécurité d'un système informatique et à identifier les vulnérabilités qui pourraient autrement être utilisées pour exploiter les systèmes. L'Ofcom, le régulateur des communications du Royaume-Uni, applique volontairement, avec les fournisseurs de télécommunications, le programme TBEST, qui est un test d'intrusion qui vise à stimuler une cyberattaque afin d'identifier les failles de sécurité qui peuvent ensuite être corrigées par un processus de correction afin d'améliorer les dispositifs de sécurité du réseau des opérateurs[20]. Le régulateur a donné un aperçu du processus et des différentes parties prenantes impliquées. Plus généralement, ce système est un exemple d'approche de régime de surveillance adoptée par l'Ofcom, qui souligne l'importance d'établir des relations de collaboration avec le secteur réglementé par l'autorité. À ce jour, tous les fournisseurs de services de communication du Royaume-Uni ont été ou sont soumis volontairement au programme TBEST et ont mis en œuvre des changements en conséquence. Ce programme n'est ni une "norme" ni un processus de certification. L'objectif est de permettre aux fournisseurs de communications de prendre conscience des cybermenaces et de mettre en œuvre les changements appropriés en temps opportun pour améliorer leurs capacités de cyberdéfense. En étant conscient de ces vulnérabilités et faiblesses et en y remédiant, l'opérateur est vraiment mieux à même de protéger ses réseaux.

Cinquième point à retenir: Des efforts sont déployés pour sensibiliser les consommateurs et les fabricants à l'importance de la cybersécurité et aux avantages de produits plus sûrs

Des efforts ont été faits pour sensibiliser le public à l'importance de la cybersécurité et aux avantages de choisir des produits plus sûrs.

Une approche dans ce sens est l'élaboration d'un système d'étiquetage de cybersécurité (CLS), dans lequel, comme dans le cas de Singapour, les produits certifiés peuvent s'accompagner d'un label. Les systèmes d'étiquetage servent principalement d'outil d'information pour les consommateurs. L'Agence de la cybersécurité de Singapour (CSA) s'est penchée sur un système d'étiquetage de la cybersécurité qui vise à aider les consommateurs à faire la distinction entre les appareils IoT plus ou moins sécurisés[21]. Le système est mis en œuvre sur une base volontaire (à l'exception des routeurs WiFi, pour lesquels il est obligatoire) et comporte quatre niveaux, le niveau 1 étant la base de sécurité. Les niveaux 1 et 2 sont fondés sur l'auto-évaluation des fabricants et les niveaux 3 et 4 impliquent une évaluation par une tierce partie, réalisée par un laboratoire approuvé. Le système est à plusieurs niveaux pour inciter les fabricants à intégrer des mesures de sécurité supplémentaires au-delà des

[18] https://isms.kisa.or.kr/main/csap/intro/index.jsp
[19] https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity
[20] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work
[21] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090016PDFE

exigences de base. La CSA a également examiné les compromis liés à l'imposition de normes de cybersécurité, y compris le risque que les fabricants court-circuitent le marché en raison de l'augmentation des coûts de mise en conformité. Au lieu de cela, l'objectif est de changer l'état d'esprit des fabricants pour voir la cybersécurité comme un catalyseur et un différenciateur du marché plutôt qu'un coût. Concernant l'impact d'un système d'étiquetage de la cybersécurité à Singapour, le processus en est encore à ses débuts et des efforts sont déployés pour encourager les fabricants à participer au programme et à améliorer leur cybersécurité. Une enquête publique sera menée à nouveau à l'avenir pour évaluer la sensibilisation et le comportement des consommateurs. Le coût de la conformité est réduit au minimum pour les fabricants aux niveaux 1 et 2, et il n'y a pas eu d'augmentation importante du coût des produits pour les consommateurs. Avec le système mis en place sur une base volontaire, les forces du marché devraient inciter les fabricants à améliorer la cybersécurité.

Au-delà des labels, il est tout aussi important d'investir dans les contrôles techniques que dans la sensibilisation et l'éducation de la population sur les risques de cybersécurité auxquels les organisations et les pays sont confrontés. Actuellement, les attaques par rançongiciel sont la tendance la plus préoccupante. Pour ce type d'attaques, le principal vecteur d'attaque – c'est-à-dire la façon dont un criminel pénètre dans un réseau ou un système – est le courrier électronique d'hameçonnage[22]. Dans ce contexte, Les cybercriminels peuvent souvent contourner les contrôles de sécurité simplement en cliquant sur un courriel d'hameçonnage. Il est donc crucial, pour garantir la cybersécurité, que les citoyens et les consommateurs soient sensibilisés à ces thèmes.

Sixième point à retenir: Il est important de rechercher des accords internationaux de synergie/d'harmonisation et de réciprocité

L'existence d'accords de réciprocité entre les modèles de garantie de la cybersécurité, à savoir les systèmes de certification et d'étiquetage, peut être un facteur déterminant pour la transposition à plus grande échelle de ces pratiques. Comme les parties prenantes l'ont souligné, les accords de réciprocité peuvent aider à faciliter la conformité pour les acteurs industriels opérant sur de multiples marchés. Toutefois, étant donné que les accords de réciprocité sont un mécanisme formel qui comporte de nombreuses contraintes nationales et dont l'approbation et la signature prennent du temps, il est nécessaire que les pratiques en matière d'assurance de la cybersécurité trouvent des synergies avec les approches internationales existantes qui sont conformes aux priorités et aux besoins nationaux. Cela réduira la charge réglementaire pesant sur les fournisseurs de produits et de services, l'objectif étant d'éviter des exigences contradictoires.

La CSA a souligné l'importance de la collaboration internationale dans l'élaboration et la mise en œuvre de son système d'étiquetage de la cybersécurité. Singapour a signé des accords de reconnaissance mutuelle avec la Finlande et l'Allemagne et s'efforce d'élargir ses partenariats dans ce domaine. Singapour a réfléchi à sa propre expérience en indiquant que les gouvernements devaient être proactifs dans l'établissement de la reconnaissance, bien que les fabricants aient également intérêt à soutenir le processus de reconnaissance car il réduit la charge de tests et de certifications répétés, ainsi que l'accès aux marchés, dans différentes juridictions. Le processus consiste à réunir les parties intéressées afin d'harmoniser les exigences et d'établir des normes communes réalistes et pas trop contraignantes.

Au niveau européen, l'Agence de l'Union européenne pour la cybersécurité (ENISA) a pour mandat d'élaborer trois systèmes de certification qui seraient reconnus dans l'ensemble du marché intérieur, et impliquerait donc une "reconnaissance mutuelle" automatique dans l'ensemble de l'Union européenne (UE). Il s'agit des éléments suivants: 1) *le système de critères communs de l'UE pour les produits TIC*, pour lequel l'acte législatif est en cours d'élaboration, en vue de son adoption; 2) *le schéma des services en nuage*, qui fait actuellement l'objet de discussions approfondies et enfin; 3) *le schéma 5G*, qui est en cours d'élaboration[23].

Outre la réciprocité et compte tenu des marchés internationaux sur lesquels opère l'industrie, l'harmonisation des exigences de base en matière de sécurité est également une considération importante. Les normes de l'ETSI sur les produits grand public IoT en sont un exemple. La principale question est de savoir dans quelle mesure les différents cadres réglementaires seront harmonisés et dans quelle mesure ils seront reliés par les mêmes normes internationales. À cet égard, il a été noté que le renforcement et même la recherche d'un cadre propice au dialogue constituaient un défi. Dans un souci d'harmonisation, les activités de l'ENISA dans le domaine de la normalisation de la cybersécurité et de la 5G nécessitent une collaboration entre le CEN, la CENELEC, l'ETSI, l'ISO, la CEI, la GSMA, le 3GPP et GlobalPlatform. L'un des principaux résultats de l'agence a été de consolider les contrôles de sécurité 5G de différentes organisations de normalisation (SDO) dans un référentiel unique[24].

[22] Tactique couramment utilisée par les cybercriminels pour inciter les gens à révéler des informations sensibles ou à télécharger des logiciels malveillants qui infectent le système/réseau pris pour cible.

[23] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090019PDFE.pdf

[24] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Annexe: Exemples de pratiques en matière d'assurance de la cybersécurité

Pays ou organisation	Nom des pratiques	Type de pratiques	Domaine d'application	Type d'approche	Référence
Australie	Orientations à l'intention des fabricants pour assurer la sécurité dès la conception pour l'Internet des objets	Orientation	Internet des objets	Volontaire	Lien
Australie	Code de pratique: Sécuriser l'Internet des objets pour les consommateurs	Code de pratique	Internet des objets	Volontaire	Lien
Brésil	Loi 77/2021 Exigences en matière de cybersécurité applicables aux équipements de télécommunication	Exigences pour le programme de certification	Équipements de télécommunication	Volontaire	Lien
Brésil	Loi 2436/2023 – Exigences minimales en matière de cybersécurité applicables aux équipements de locaux d'abonnés (CPE)	Exigences pour le programme de certification	CPE	Volontaire	Lien
Royaume d'Arabie saoudite	Vérification et validation indépendante (IV&V)	Test et certification des produits. Recensement et classification des dispositifs et logiciels	Produits	Volontaire dans un premier temps	Lien
Corée (République de)	Programme d'assurance de la sécurité du nurage (CSAP)	Programme de certification	Nuage	Combiné – volontaire au niveau général. Obligatoire pour la fourniture de services de nuage aux organismes publics.	Lien
Singapour	Système d'étiquetage de la cybersécurité	Système de certification et d'étiquetage	Internet des objets	Combiné – volontaire au niveau général. Obligatoire pour les routeurs WiFi domestiques	Lien
Royaume-Uni de Grande-Bretagne et d'Irlande du Nord	Régime applicable à la sécurité des produits et à l'infrastructure des télécommunications (Sécurité des produits)	Exigences minimales en matière de sécurité	Produits connectés	Obligatoire	Lien
Royaume-Uni de Grande-Bretagne et d'Irlande du Nord	Programme TBEST	Test d'intrusion	Réseaux de télécommunication	Volontaire	Lien

ITUPublications
Publié en Suisse, Genève, 2023

Union internationale des télécommunications
Place des Nations, CH-1211 Genève Suisse