ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité » n°66
Lundi 26 février 2024

La cyber-résilience dans l'Union Européenne, il est temps d'agir !

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 1 Cybersécurité et E-santé
clarisse.veron@etu.u-paris.fr

SOMMAIRE

Introduction

La conférence du "Lundi de la Cybersécurité", dans sa session de février 2024, s'est penchée sur la thématique cruciale de la cyber-résilience, une faculté vitale dans notre paysage numérique en perpétuelle évolution. Cette conférence, orchestrée par des sommités telles que Laurent Peliks, Stéphane Brebion et Maître Olivier Iteanu, a servi de tremplin pour la discussion approfondie sur l'alignement des systèmes d'information avec les capacités de récupération du vivant face aux adversités.

Objectif de la Conférence :

Cette conférence avait pour but premier de souligner la cyber-résilience comme pierre angulaire de la sécurité informatique moderne. Elle a exploré la capacité des structures à anticiper, contrecarrer et se relever des cyberattaques, reflétant l'importance des réglementations européennes récentes dans la mise en place d'une défense numérique stratégique et coordonnée.

Contexte et Intervenants :

Dans un monde où la menace des cyberattaques s'intensifie, la conférence a mis l'accent sur le rôle des réglementations telles que la directive NIS2, la loi le règlement DORA et la loi CRA pour bâtir une résilience efficace. Les intervenants, dotés d'expertises variées, ont apporté des éclaircissements sur les défis et les solutions dans le domaine de la cyber-résilience, tout en insistant sur la nécessité d'une synergie entre sensibilisation, technologie et réglementation.

I. Introduction à la Cyber Résilience

La première partie de la conférence animée par Laurent Peliks a abordé plusieurs thèmes clés autour de la cyber-résilience, en mettant en lumière les définitions, le cadre d'action, les enjeux et les réglementations européennes pertinentes.

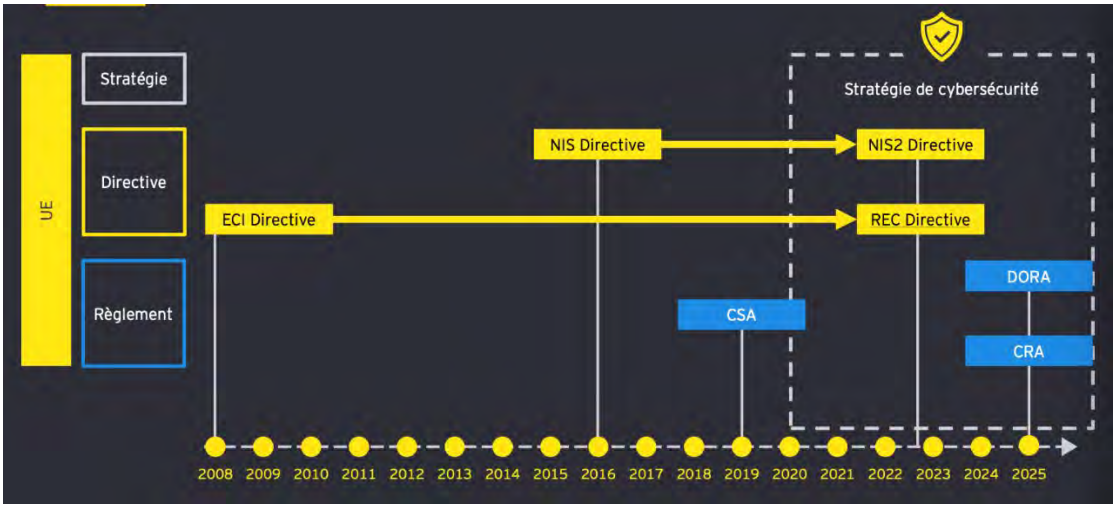
L'orateur a ouvert le dialogue en définissant la cyber-résilience, la présentant comme la capacité d'une organisation à anticiper, se préparer, répondre et s'adapter à divers incidents cybernétiques, tout en mettant en avant l'importance de tirer des leçons des expériences passées pour améliorer les stratégies de sécurité de manière continue. Il a souligné le contexte actuel marqué par une augmentation des cyberattaques, et la nécessité d'une sensibilisation accrue et d'une préparation adéquate face à des menaces de plus en plus sophistiquées. Mr Laurent Peliks a souligné l'importance de considérer la cyber-résilience non seulement en termes de prévention des attaques mais aussi en termes de capacité à maintenir des opérations critiques lors d'incidents, en visant une récupération efficace et rapide.

Un framework complet pour la cyber-résilience a été présenté, englobant la préparation, la résistance, la récupération, et l'adaptation. Ce cadre souligne l'importance d'une surveillance constante du paysage des menaces, d'une évaluation précise du risque, et d'une planification stratégique pour la continuité des activités.

Les enjeux de la cyber-résilience ont mis en évidence les défis contemporains auxquels les organisations sont confrontées, notamment la complexité croissante des cyberattaques et la nécessité d'une réponse coordonnée impliquant à la fois des aspects technologiques et humains. La discussion a porté sur l'importance de la culture de la sécurité au sein des organisations,

l'implication des directions générales, et la gestion des crises en tant qu'éléments fondamentaux pour renforcer la cyber-résilience.

Enfin, les réglementations européennes ont été abordées par Mr Laurent Peliks, avec un accent particulier sur les directives NIS2, DORA, et CRA, qui visent à établir un cadre légal pour améliorer la cyber-résilience à travers l'Union européenne. Ces réglementations soulignent l'importance de la protection des infrastructures critiques, la nécessité pour les secteurs financiers et autres industries clés de se conformer à des normes de sécurité élevées, et l'encouragement à une collaboration plus étroite entre les États membres pour partager les informations et meilleures pratiques en matière de cybersécurité.



Cette partie de la conférence a donc mis en lumière le besoin crucial pour les organisations de développer une approche holistique et intégrée en matière de cyber-résilience, en prenant en compte les défis technologiques, humains, et réglementaires.

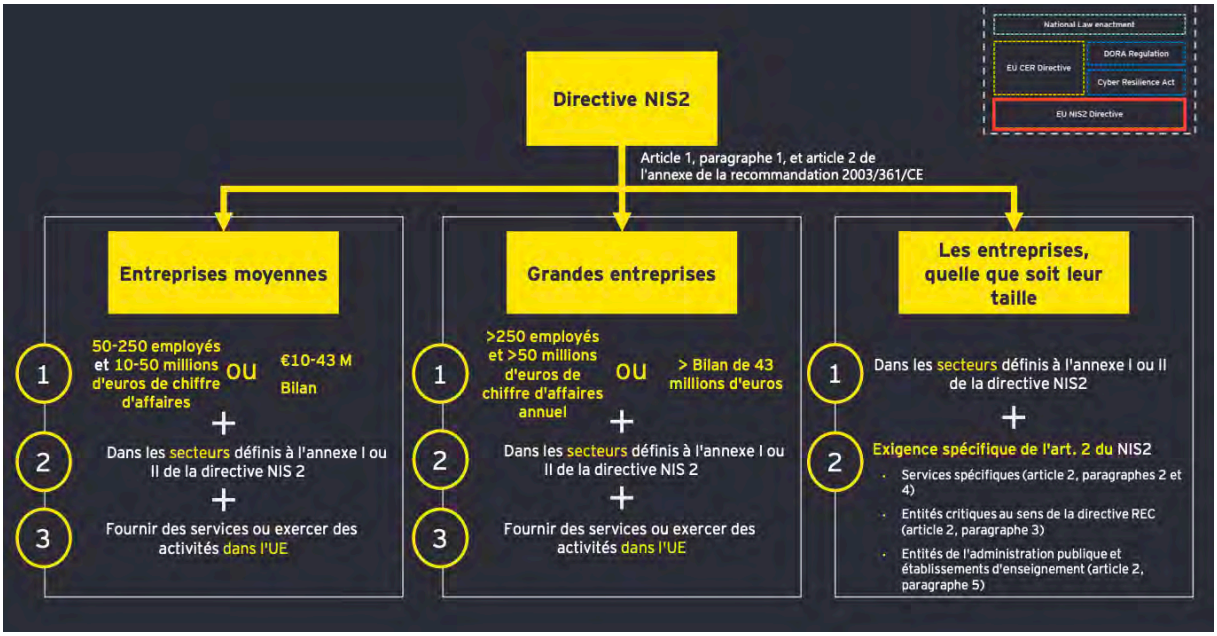
II. Règlementation Européenne : introduction à NIS2 du point de vue opérationnel (exigences cyber)

Dans cette deuxième partie, Stéphane Brebion nous introduit la réglementation européenne, en mettant l'accent sur l'introduction à NIS2 du point de vue opérationnel, notamment sur les exigences en matière de cybersécurité.

Il explique que la stratégie de cybersécurité européenne s'appuie principalement sur la directive NIS2, qui établit un cadre renforcé pour la sécurité des réseaux et des systèmes d'information au sein de l'UE. Cette directive vise à augmenter le niveau de protection cybernétique des organisations concernées, en particulier les entreprises importantes et les entreprises essentielles.

Mr Brebion souligne l'importance de comprendre les implications de NIS2, qui s'inscrit dans un ensemble plus large de réglementations européennes telles que le Cyber Resilience Act (CRA) et DORA, ce dernier se concentrant exclusivement sur le secteur financier. Ces réglementations cherchent à harmoniser les pratiques de cybersécurité et à améliorer la résilience des systèmes d'information à travers l'Europe.

La directive NIS2, en particulier, élargit considérablement le périmètre d'application par rapport à son prédécesseur, NIS1, et introduit des mesures spécifiques pour renforcer la sécurité de la chaîne d'approvisionnement. Mr Brebion met en évidence trois piliers fondamentaux de NIS2 : l'identification des systèmes critiques, l'implémentation d'un cadre de contrôle conforme à l'état de l'art pour la gestion des risques, et l'évaluation continue de la sécurité des systèmes critiques.



Il aborde ensuite les critères qui définissent les entités concernées par NIS2, en fonction de leur taille et de leur secteur d'activité, et met l'accent sur l'importance de la gestion des risques de cybersécurité. Les entités doivent prendre des mesures appropriées pour prévenir et minimiser l'impact des incidents de sécurité, corriger rapidement les non-conformités et signaler tout incident significatif.

Stéphane Brebion conclut en soulignant les défis et les opportunités que NIS2 présente pour les organisations en Europe. Il insiste sur la nécessité d'une mise en œuvre efficace et d'une coopération accrue entre les États membres pour garantir une cybersécurité robuste et résiliente à l'échelle de l'UE. La directive NIS2, avec son approche harmonisée et ses exigences renforcées, est vue comme un pas important vers une Europe plus sûre sur le plan cybernétique.

III. Directive NIS2 : Contrôles, sanctions et responsabilité

La troisième partie de la conférence, présentée par Maître Olivier Iteanu, s'est concentrée sur les aspects de contrôles, sanctions, et responsabilités découlant de la Directive NIS2, mettant en lumière l'évolution significative dans la réglementation de la cybersécurité au sein de l'Union européenne. Cette présentation a abordé la complexité croissante des textes réglementaires en matière de cybersécurité, soulignant la difficulté pour le grand public de naviguer dans ce labyrinthe législatif.

Maître Iteanu a d'abord rappelé le contexte qui a mené à l'adoption de ces directives et règlements, notamment la dépendance accrue au numérique, la multiplication des cyberattaques, l'externalisation des services, et une faible élucidation des cybercrimes due aux limites juridictionnelles nationales. Ces éléments soulignent la nécessité d'un changement de

paradigme dans la gestion de la cybersécurité, passant d'une logique punitive individuelle à une responsabilité collective et organisationnelle en matière de sécurité numérique.

Dans ce nouveau cadre, les organisations sont tenues à des obligations positives, incluant la mise en œuvre de mesures techniques, organisationnelles, et fonctionnelles pour assurer un niveau adéquat de sécurité. La Directive NIS2, en particulier, met l'accent sur ces obligations, exigeant des entités concernées qu'elles évaluent et gèrent les risques, et qu'elles notifient les incidents de sécurité aux autorités compétentes dans des délais définis. L'échec à respecter ces obligations peut entraîner des sanctions administratives significatives, soulignant ainsi l'importance d'une approche proactive en matière de cybersécurité.

Les sanctions prévues par la Directive NIS2 sont substantielles, pouvant atteindre jusqu'à 2% du chiffre d'affaires mondial pour les entités essentielles, et jusqu'à 1,4% pour les entités importantes, illustrant la sévérité des conséquences en cas de non-conformité. Cette approche s'inscrit dans la lignée du RGPD, qui avait déjà introduit des sanctions financières lourdes pour encourager les organisations à protéger les données personnelles.

Maître Iteanu a également abordé le sujet de la responsabilité légale, notant qu'au-delà des sanctions administratives, les organisations pourraient faire face à des actions en responsabilité de la part de tiers lésés par une défaillance de sécurité. Cette perspective renforce la nécessité pour les organisations de non seulement se conformer aux exigences réglementaires mais aussi d'adopter une culture de sécurité intégrée à tous les niveaux de l'organisation.

En conclusion, cette partie de la conférence a mis en exergue la Directive NIS2 comme un tournant majeur dans la réglementation de la cybersécurité en Europe, marquant un passage à une responsabilisation accrue des organisations dans la protection contre les cybermenaces. Le changement de paradigme souligné par Maître Iteanu appelle à une mobilisation générale pour une meilleure résilience numérique, reflétant la prise de conscience de l'importance cruciale de la sécurité informatique dans notre société interconnectée.

IV. Suite des réglementations européennes en matière de cyber résilience : REC, CRA, DORA

Dans la quatrième partie de la conférence, Stéphane Brebion a repris l'exposé pour aborder les réglementations européennes en matière de cyber résilience, mettant l'accent sur les directives REC (Résilience des Entités Critiques), CRA (Cyber Resilience Act), et le règlement DORA (Digital Operational Resilience Act). Cette partie a souligné l'importance de ces réglementations dans le renforcement de la sécurité et de la résilience des infrastructures critiques, des produits numériques, et du secteur financier au sein de l'UE.

La directive REC vise à améliorer la résilience des entités fournissant des services essentiels, en se concentrant particulièrement sur la sécurité physique tout en couvrant également certains aspects numériques. Elle introduit la notion d'entités critiques, qui, comme dans NIS2, sont essentielles au maintien de fonctions sociétales vitales ou d'activités économiques. Les exigences principales de REC incluent l'évaluation des risques, la mise en œuvre de mesures de résilience, et le reporting obligatoire en cas d'incidents significatifs. Les sanctions et la mise en application de ces mesures seront définies par chaque État membre, avec une période de transposition prévue jusqu'en octobre 2024.

Le CRA se concentre exclusivement sur la cybersécurité des produits numériques, visant à établir un cadre pour la sécurité dès la conception et tout au long du cycle de vie des produits. Cette réglementation exige des fabricants qu'ils évaluent les risques de sécurité, signalent les vulnérabilités, et assurent une diligence raisonnable avant la mise sur le marché. Les amendes pour non-conformité peuvent atteindre jusqu'à 15 millions d'euros ou 2,5% du chiffre d'affaires annuel mondial. Le CRA, actuellement en projet de loi, prévoit une période de transition de 24 mois, avec une entrée en vigueur attendue vers fin 2025.

DORA spécifie les exigences en matière de résilience opérationnelle pour le secteur financier, complétant et modifiant NIS2 pour répondre aux particularités de ce secteur. L'objectif est d'harmoniser les mesures de sécurité et de gestion des risques à l'échelle européenne, en mettant l'accent sur la supervision centralisée, le reporting des incidents, et le partage d'informations. DORA couvre les banques, les institutions de crédit, les compagnies d'assurance, et d'autres entités financières, imposant une gouvernance rigoureuse des risques liés aux TIC, des tests de résilience, et une communication efficace en cas d'incident.

Face à la complexité et à la portée de ces réglementations, les organisations doivent adopter une approche structurée pour se conformer. Cela comprend le cadrage des textes de loi, l'identification des périmètres concernés, la réalisation de diagnostics pour évaluer l'impact des exigences, et l'élaboration de plans d'action pour la mise en conformité. Le maintien de cette conformité dans le temps est crucial, nécessitant une veille constante sur l'évolution des menaces et des standards de sécurité.

Cette partie de la conférence a donc fourni un aperçu complet des efforts entrepris par l'Union européenne pour renforcer la cyber résilience à travers divers secteurs, soulignant l'importance d'une approche proactive et intégrée pour la sécurité numérique.

V. Séance de Questions - Réponses

Question : Je ne vois rien sur la robustesse des infrastructures, les OS et le réseau sont-ils acceptés avec leurs faiblesses « structurelles » comme telles ?

→ La réponse de Mr Laurent Peliks aborde la question de la robustesse des infrastructures informatiques, y compris les systèmes d'exploitation (OS) et les réseaux, et leur acceptation avec leurs éventuelles faiblesses structurelles. Elle met en lumière la responsabilité des entités de sécuriser leurs systèmes d'information essentiels ou critiques contre les menaces telles que les codes malveillants, tout en gérant les configurations de sécurité de manière adéquate. La discussion englobe également le rôle des fournisseurs et des éditeurs de logiciels, y compris ceux qui ne sont pas basés dans l'Union européenne, et comment ces derniers s'intègrent dans le cadre réglementaire européen, notamment en ce qui concerne les services numériques essentiels.

Le débat porte également sur des sujets tels que la territorialité, la souveraineté, et la conformité avec des réglementations spécifiques comme le RGPD, soulignant l'importance de la localisation des données et des implications potentielles en termes de sanctions. Cela indique la complexité et l'importance croissante de ces questions dans le paysage actuel de la sécurité informatique et de la conformité réglementaire.

Question : Quand les éditeurs de logiciel seront-ils rendus responsables des conséquences des failles de sécurité qui restent dans leurs outils ?

→ Maître Olivier Iteanu aborde la question de la responsabilité des éditeurs de logiciels concernant les failles de sécurité dans leurs produits. Il souligne que les éditeurs sont déjà, dans une certaine mesure, tenus responsables si une faille de sécurité significative, qui représente un manquement évident aux règles de l'art, est présente dans leur logiciel. Il n'y a pas d'obligation de sécurité absolue, mais en cas de négligence manifeste menant à une faille béante, une action en responsabilité peut être engagée.

Cette responsabilité n'est pas une nouveauté introduite par des textes récents mais s'inscrit dans un cadre juridique existant qui permet d'engager la responsabilité des éditeurs en cas de failles de sécurité majeures. Dans le secteur des logiciels métiers ou des solutions à enjeux importants, il est courant de voir des actions engagées contre les éditeurs, souvent résolues en privé, avec l'intervention d'assurances et de négociations entre avocats.

Maître Olivier Iteanu compare cette situation à l'impact du RGPD, qui a grandement sensibilisé le public aux enjeux de protection des données personnelles. Il anticipe un effet similaire avec la directive NIS 2, notamment en ce qui concerne la lutte contre les fraudes à l'identité, un des actes de cybercriminalité les plus répandus. Ces textes législatifs contribuent à élever le niveau général de compétence en matière de cybersécurité et d'identité numérique.

Il conclut que, bien que des actions contre des éditeurs majeurs comme Microsoft puissent être compliquées en raison de barrières juridiques, il est possible d'engager la responsabilité des éditeurs pour des failles de sécurité. Cela fait partie d'une évolution plus large vers une meilleure compréhension et gestion des risques numériques, nécessitant une adaptation et une application réfléchies des cadres législatifs existants.

Question : Les sanctions définies par les États s'appliquent-t-elles aux sociétés domiciliées en Irlande (gafam) ?

→ La réponse indique que l'objectif de la réglementation européenne est de s'assurer que tous les acteurs du marché unique, y compris les sociétés domiciliées en Irlande, contribuent à la cybersécurité et à la cyber résilience. Cela suggère que les sanctions définies par les États membres de l'UE, y compris pour les entreprises du GAFAM, s'appliquent si elles opèrent au sein de l'Union européenne.

Question : Le fait de faire de l'ANSSI un outil de sanction ne va-t-elle pas changer la relation que beaucoup d'entreprises ont avec elle ?

→ L'orateur reconnaître qu'il y a un défi potentiel dans le rôle double de l'ANSSI, qui est à la fois un organe de conseil et de sanction. La mention des "formations restreintes" au sein d'organismes comme la CNIL illustre une manière de séparer les fonctions d'accompagnement et de sanction pour préserver l'indépendance et l'objectivité nécessaire lorsqu'il s'agit d'imposer des sanctions.

Question : Le cloud pourrait améliorer la résilience de petites entités qui n'ont pas de ressources permanentes. Cet état de modèle in/off du cloud vient complexifier la répartition des

responsabilités, en particulier pour la gestion des tenants et leurs accès. Comment envisagez-vous la résilience des écosystèmes ?

→ Le cloud offre effectivement une opportunité d'amélioration de la résilience pour les petites entités qui n'ont pas de ressources permanentes. En ce qui concerne la complexité et la répartition des responsabilités, notamment pour la gestion des tenants et de leurs accès, il est crucial de développer une stratégie de résilience des écosystèmes adaptée.

En France, par exemple, l'ANSSI encourage la certification des services cloud, visant à responsabiliser les fournisseurs de services cloud, et cela ne s'adresse pas exclusivement aux grands éditeurs, mais aussi à des sociétés plus petites qui s'engagent vers l'utilisation du cloud. La principale difficulté pour les PME réside dans le fait qu'elles sont souvent confrontées à des contrats d'adhésion standardisés, qui sont la norme chez les fournisseurs de services cloud. Ces PME nécessitent donc une réglementation impérative plus robuste que les contrats pour être protégées.

Dans ce contexte, des réglementations telles que le RGPD jouent un rôle clé. Un fournisseur de services cloud ne peut pas contractuellement aller à l'encontre des dispositions impératives du RGPD. Cela offre un cadre de protection pour les entités utilisatrices du cloud. En outre, avec l'anticipation de la transposition de la directive NIS 2 et le règlement eIDAS (Règlement sur l'identification électronique et les services de confiance), on voit une tendance à renforcer les réglementations impératives qui prévalent sur les contrats d'adhésion.

Ces mesures sont d'autant plus pertinentes que dans l'écosystème du cloud, les contrats d'adhésion sont souvent les seuls documents contractuels disponibles, même pour les grandes entités qui se trouvent sans marge de manœuvre pour les négocier. Ainsi, la législation européenne et nationale joue un rôle déterminant pour assurer la résilience et la protection des petites et moyennes entreprises dans l'univers du cloud.

Question : Qu'est-ce qu'un produit numérique pour la réglementation CRA ?

→ Un produit numérique, selon la réglementation CRA, inclut à la fois le matériel et le logiciel qui incorporent des éléments numériques. Cela peut inclure des exemples tels que des capteurs intelligents, des caméras intelligentes, des appareils mobiles, des appareils réseau, et d'autres composants liés à l'écosystème numérique. En outre, les solutions SaaS (Software as a Service) qui agrègent des données et qui, dans certains cas, peuvent contrôler ces différents matériels, sont également incluses et considérées comme des produits numériques au sens de cette réglementation. Ces produits sont donc soumis à la réglementation CRA en raison de leur capacité à interagir avec ou à être composés d'éléments numériques.

Question : Quelles sont les limites des tests de résiliences ?

→ Les tests de résilience ne sont pas seulement une affaire de technologie (IT) mais impliquent également une compréhension et une intégration des processus métiers. Cela peut constituer une limite si les tests ne couvrent pas adéquatement les aspects métiers ou s'ils ne sont pas alignés sur les besoins réels de l'entreprise.

Il est également mentionné que bien que les tests de résilience progressent, la maturité optimale n'est pas encore atteinte. Cela peut suggérer que les tests actuels peuvent ne pas être

suffisamment développés pour simuler avec précision ou réagir à des scénarios de crise complexes ou nouveaux.

L'accent est mis sur la reprise des données et la gestion des données dans les tests de résilience, ce qui implique que les limites peuvent également résider dans la capacité à restaurer les opérations et les informations critiques après une perturbation.

La discussion sur le nombre d'entreprises affectées par la directive NIS2 indique une préoccupation quant à l'étendue de l'application des tests de résilience et si elles sont réalistes ou faisables pour toutes les entreprises concernées, surtout au niveau européen.

Conclusion

Pour conclure, ce Lundi de la Cybersécurité du mois de février 2024 a été une exploration approfondie de la cyber-résilience, mettant en exergue l'importance cruciale de préparer les systèmes d'information face aux menaces cybernétiques en constante évolution. Les discussions menées par des experts tels que Laurent Peliks, Stéphane Brebion, et Maître Olivier Iteanu ont révélé une compréhension commune de la nécessité d'une approche holistique intégrant la technologie, la sensibilisation, et la réglementation pour bâtir une défense numérique robuste.

Les insights partagés lors de cette conférence soulignent l'importance de l'alignement avec les réglementations européennes récentes, illustrant un paysage où la cyber-résilience devient la pierre angulaire de la sécurité informatique moderne. Ce forum a non seulement enrichi la connaissance collective mais a également pavé la voie à une collaboration étroite entre les différentes entités pour renforcer la sécurité numérique face à un avenir incertain.