sosafe

Les détails de la directive SRI2 (NIS2) : ce que cela implique pour votre société

> Découvrez les dispositions de la directive SRI2 (NIS2) pour contrer la sophistication croissante des menaces cyber

SRI2 (NIS2)

La directive sur la sécurité des réseaux et des systèmes d'information est un texte juridique destiné à assurer un niveau élevé commun de cybersécurité chez tous les États membres de l'Union européenne. Elle vise à protéger les secteurs critiques en imposant des normes plus strictes, ainsi qu'en favorisant un signalement rapide des incidents et une plus grande collaboration en matière de sécurité.

Contenu

Qu'est-ce que la directive SRI2 ?

La directive SRI2, également connu sous le nom de NIS2, remplace la première directive sur la sécurité des réseaux et des systèmes d'information. Elle s'impose comme un élément central de la législation visant à **renforcer la cybersécurité et à protéger les infrastructures essentielles dans toute l'Union européenne (U.E.)**. En comblant les lacunes de la précédente directive et en élargissant son champ d'action, SRI2 renforce les dispositions en matière de sécurité, resserre les obligations de signalement et améliore les capacités de gestion de crise.

Pour bien comprendre la nécessité et l'utilité de la directive SRI2, il faut avoir une bonne vue d'ensemble de notre écosystème de plus en plus interconnecté. L'infrastructure numérique européenne est complexe et tentaculaire. Elle prend en charge presque toutes les facettes du commerce et de la vie quotidienne d'aujourd'hui. Une telle interconnectivité offre des opportunités de croissance et d'efficacité exceptionnelles, mais ouvre aussi la porte à une multitude de menaces cyber et de vulnérabilités potentielles.

En consolidant les protections numériques mises en place avec la directive SRI de 2016 et en étendant sa portée, SRI2 constitue une place forte dans notre paysage cybernétique. Votée en 2022, **cette nouvelle directive est une réponse à la prolifération de menaces cyber de plus en plus sophistiquées et dangereuses** et définit une stratégie de défense solide, complète et modulable.

État de la situation en matière de menaces cyber en Europe : pourquoi SRI2 ?

Le paysage des menaces a récemment pris un tournant dramatique. Les hackers ne cessent de se perfectionner et d'innover. Les progrès de la technologie, en particulier ceux de l'IA, jouent un rôle majeur dans cette mutation puisqu'ils permettent aux cybercriminels d'échafauder des plans plus sophistiqués et infaillibles. Dans un contexte où le marché juteux du piratage ne cesse de se professionnaliser, il n'a jamais été aussi simple de perpétrer des attaques. Les acteurs malveillants ont même à leur disposition des plateformes fonctionnant sur le même modèle que les offres SaaS classiques.

À cette situation déjà complexe s'ajoutent les tensions mondiales et les conflits internationaux qui se répercutent de plus en plus dans le cyberespace : piratages commandités par des États, cyberespionnage et guerre cybernétique sont aujourd'hui des armes puissantes qui enveniment la situation et intensifient les menaces. En outre, l'essor du télétravail a, sans le vouloir, servi la cause des criminels, leur ouvrant de nouvelles opportunités pour exploiter des vulnérabilités telles que des appareils personnels ou des connexions non sécurisés.

Notre Analyse du risque humain 2023 a confirmé ces tendances : **3 professionnels de la cybersécurité sur 4 pensent que les risques auxquels est exposée leur entreprise ont augmenté avec l'accumulation de ces différents facteurs : les crises géopolitiques, l'avènement de l'IA et le passage massif au télétravail**. D'ailleurs, une société sur deux a été victime d'une cyberattaque. Plus alarmant encore : un tiers des professionnels pense que leur structure subira une autre attaque dans un futur proche.

Ce déferlement de menaces cyber constitue particulièrement un danger pour les infrastructures essentielles. Celles-ci attisent les convoitises des cybercriminels : dans la mesure où une interruption de leurs services nécessiterait une intervention d'urgence, ces secteurs sont susceptibles d'être plus vulnérables au chantage de personnes malveillantes motivées par l'appât du gain. Les données publiées par Statista en 2022 soulignent ces points faibles et montrent que l'énergie, l'enseignement, la santé, les instances gouvernementales, les transports et les médias/télécommunications comptent parmi les secteurs les plus ciblés par les cyberattaques.

Les mesures réglementaires comme la directive SRI2 et DORA sont nées du constat que la situation a atteint une ampleur sans précédent. Dans ce contexte troublé, elles cherchent à guider les entités européennes sur la voie de la sécurité. Leur but premier est de promouvoir une réponse harmonisée, en veillant à ce que les structures soient mieux équipées pour contrecarrer ces menaces en perpétuelle évolution.

Quels sont les objectifs de SRI2 ?

SRI2 repousse les limites de la résilience numérique et de la gestion des menaces. Loin de se contenter d'augmenter la cybersécurité d'un cran, elle propose une feuille de route complète pour assurer la continuité des activités, renforcer les collaborations et favoriser l'émergence d'un personnel bien au fait des principes à appliquer pour naviguer en toute sécurité. Dans cette optique, la directive SRI2 s'est fixé les objectifs suivants :

Mise en œuvre de bonnes pratiques pour la gestion des actifs afin d'identifier et de protéger les actifs et les systèmes d'information critiques

Définition et mise en œuvre de stratégies de cybersécurité et de protocoles de gestion des risques

Élaboration d'une stratégie pour **garantir la continuité des services critiques** en cas de cyberincidents

Formation et sensibilisation renforcée parmi les employés pour leur enseigner les protocoles les plus efficaces en matière de cybersécurité

Suppression des incohérences et amélioration de la communication et de la collaboration entre États membres

Signalement aux autorités compétentes et entretien des capacités de réponse en cas d'incident

Mise en place de protocoles pour la gestion des incidents, de mandats de signalement et de plans d'intervention

Implémentation de mesures de sécurité au niveau de la chaîne d'approvisionnement, visant à contrôler et garantir la sécurité des prestataires tiers de services

Contrôle du signalement des incidents aux organismes adaptés et entretien des capacités de réponse en cas d'incident

De SRI à SRI2 : qu'est-ce qui change ?

La directive SRI d'origine, aussi connu sous le nom NIS, réagissait à l'essor de la numérisation qui entraînait son lot de risques cyber, un danger nouveau, menaçant autant les sociétés que le grand public, et qu'il fallait prendre au sérieux. Une réponse était nécessaire, face à ces menaces, pour protéger les services essentiels, les informations sensibles et le bien-être des personnes et des économies. Cependant, lorsque la directive SRI a été transposée dans le droit interne des États membres en 2018, il s'est avéré que sa mise en application variait selon les pays, générant un système fragmenté dans lequel les sociétés n'avaient pas implémenté les exigences ou ne l'avaient fait que partiellement. Ces inégalités étaient notamment dues au fait que la définition d'un service essentiel diffère d'un État à l'autre. Il devenait donc indispensable de proposer une nouvelle loi, plus détaillée et plus forte.

Face à la nécessité de réviser la directive SRI, la Commission européenne a publié une nouvelle directive SRI2 qui s'adapte aux besoins actuels du marché et comble les lacunes du texte précédent. Pour être plus précis, **la directive SRI2 étend le périmètre** des entités désignées comme prestataires de services essentiels, définit une nouvelle organisation des intermédiaires en cas de crise, ainsi que des obligations de signalement plus strictes pour les structures. Elle se penche aussi sur la sécurité de la chaîne d'approvisionnement et les exigences en matière de cyberhygiène, instaure des évaluations par les pairs pour renforcer la collaboration entre États membres et relève le niveau de responsabilité des organes de direction. Vous trouverez ci-après de plus amples informations sur ces changements.

Nouvelles entités et secteurs concernés

La portée de la directive SRI2 s'élargit pour inclure de nouvelles entités et des secteurs comme la production chimique, la fabrication de dispositifs médicaux, la transformation des denrées alimentaires et les services de réseaux sociaux qui jusqu'ici n'avaient pas été concernés par la directive SRI précédente. Dans son article 3, la directive SRI 2 précise les différentes catégories. Les termes « opérateur de services essentiels » et « fournisseur de service numérique » ont été remplacés par « entités essentielles » et « entités importantes » selon leur portée et leur secteur. Bien que ces différentes catégories soient soumises à des obligations similaires, les entités essentielles feront l'objet de contrôles réglementaires plus rigoureux et de mesures coercitives plus strictes. Vous trouverez plus loin une liste exhaustive des entités entrant dans le périmètre d'application de la directive SRI2.

Le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe)

Selon l'article 16, la Commission instituera un réseau EU-CyCLONe composé de représentants des autorités des États membres chargées de la gestion des crises de cybersécurité, ainsi que, lorsque c'est nécessaire, de représentants de la Commission européenne. L'objectif principal de cet organe est d'assurer la gestion coordonnée des incidents de cybersécurité majeurs au niveau des différents pays en :

- S'assurant que les pays sont bien préparés en cas d'incidents de cybersécurité ou de crises majeurs ;
- Développant une compréhension mutuelle de ce qu'il se passe durant ces incidents et ces crises ;
- Évaluant l'impact de ces incidents et en suggérant des méthodes d'amélioration ;
- Coordonnant la gestion de ces incidents entre nations et en aidant les responsables politiques à prendre des décisions à ce sujet ;
- Échangeant sur les plans de réponse en cas d'incidents de cybersécurité et en aidant chaque pays à les mettre sur pied.

La directive SRI2 prévoit aussi la création d'un groupe de coopération pour faciliter les échanges d'informations et la coopération entre États membres. Le réseau EU-CyCLONe signalera régulièrement à ce groupe de coopération les principaux incidents et tendances de cybersécurité, notamment ceux qui affectent des organismes ou des services essentiels. Le 17 juillet 2024 et tous les 18 mois par la suite, EU-CyCLONe soumettra au Parlement européen et au Conseil un rapport détaillant ses récents travaux.

Sécurité des chaînes d'approvisionnement

L'article 22 de la directive SRI2 exige des entités qu'elles puissent répondre de la sécurité dans leur propre chaîne d'approvisionnement, y compris des risques engendrés par leurs relations avec leurs fournisseurs. Ce point est essentiel, car il s'avère que de nombreuses cyberattaques exploitent les vulnérabilités de prestataires de services tiers. Il faut donc que les sociétés évaluent la qualité et la résilience des produits et des services auxquels elles ont recours pour s'assurer qu'elles n'introduiront pas de faiblesse dommageable à des services essentiels. Il est également important que les entités analysent les mesures mises en place par leurs prestataires de services tiers pour gérer la cybersécurité afin d'évaluer si elles sont suffisantes pour protéger l'intégralité de la chaîne d'approvisionnement.

Les entités qui fournissent des services importants aux États membres - les fournisseurs de services DNS, les registres de noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centre de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux – mais résident hors de l'Union européenne doivent désigner un représentant en Europe qui sera chargé d'assurer la conformité de la structure aux obligations de la directive SRI2 et de signaler les incidents de sécurité.

Pour assurer un niveau élevé commun de cybersécurité chez tous les fournisseurs et limiter les risques de cyberincidents, les prestataires de services essentiels sont tenus d'inclure les mesures requises dans les contrats qu'ils passent avec des prestataires tiers.

Des signalements plus stricts

Pour garantir une prompte réaction, l'article 23 de la directive SRI2 exige des organismes concernés qu'ils envoient une notification à leur centre de réponse aux incidents de sécurité informatique (CSIRT) ou à une autorité nationale compétente, le cas échéant, dans les 24 heures suivant la survenue d'un incident significatif, c'est-à-dire ayant causé une perturbation opérationnelle grave des services ou des pertes financières pour l'entité ou ayant affecté d'autres personnes en causant des dommages matériels ou immatériels. Si nécessaire, les structures peuvent également demander de l'aide pour prendre des mesures d'atténuation appropriées. En réponse à cette notification, les autorités compétentes fourniront des conseils pour la gestion de l'incident et informeront les autres pays concernés, le cas échéant.

Dans un délai de 72 heures après avoir eu connaissance de l'incident, l'entité concernée apportera des détails sur l'incident, ainsi qu'une évaluation initiale. Enfin, au plus tard un mois après la présentation de la notification d'incident, elle devra soumettre un rapport comprenant une description détaillée de la gravité de l'incident, de son impact, des causes profondes à l'origine de son déclenchement et des mesures d'atténuation appliquées.

Cyberhygiène

Alors que les menaces cyber gagnent en complexité et en sophistication, il est essentiel que les différents organismes adoptent un minimum de cyberhygiène. Dans l'optique de poser des fondements pour protéger la sécurité des infrastructures essentielles, les entités doivent adopter une

base commune de pratiques incluant les mises à jour logicielles et matérielles, les changements de mot de passe, la gestion de nouvelles installations, la restriction des comptes d'accès de niveau administrateur et la sauvegarde de données.

En outre, compte tenu du nombre croissant de dispositifs connectés qui sont utilisés dans les cyberattaques, la formation et la sensibilisation des employés et des utilisateurs aux menaces cyber les plus communes sont essentielles pour poser un cadre proactif et améliorer la sécurité globale des prestataires de services essentiels au sein de l'U.E.

> **Introduction (89)** Les entités essentielles et importantes devraient adopter une vaste gamme de pratiques de cyberhygiène de base, comme les principes « confiance zéro », les mises à jour de logiciels, la configuration des dispositifs, la segmentation des réseaux, la gestion des identités et des accès ou la sensibilisation des utilisateurs, organiser une formation pour leur personnel et sensibiliser aux cybermenaces, au hameçonnage ou aux techniques d'ingénierie sociale.

Évaluations par les pairs

Comme le prévoit l'article 19 de la directive SRI2, le groupe de coopération établira un système d'évaluation volontaire par les pairs pour permettre aux États membres de tirer des enseignements des expériences partagées et de renforcer ainsi leur cybersécurité. Les évaluations par les pairs porteront sur plusieurs points, tels que le niveau de mise en œuvre des mesures de gestion des risques en matière de cybersécurité dans les différents pays, les capacités de leurs autorités compétentes et le niveau d'assistance mutuelle et de partage d'informations.

Elles pourront être effectuées sur place ou de manière virtuelle selon un code de conduite pré-établi et avec l'entière collaboration des parties impliquées. Après avoir mené à bien une telle évaluation, les experts rédigeront des rapports contenant les résultats de leurs observations et des recommandations pour améliorer la cybersécurité. Ces rapports seront soumis au groupe de coopération ainsi qu'au réseau de cybersécurité concerné, et pourront être rendus publics si l'entité évaluée le souhaite.

Responsabilité des organes de direction

Les États membres doivent définir les amendes et les sanctions imposées aux structures n'ayant pas mis en œuvre les mesures exigées par la directive SRI2. Ils devront en notifier la Commission d'ici 2025. L'article 20 de la directive SRI2 établit également la responsabilité des organes de direction, tels que les conseils d'administration ou les cadres dirigeants des entités qui ne respectent pas les exigences en matière de cybersécurité. Tout manquement à la conformité peut entraîner différentes mesures coercitives et l'imposition d'amendes conséquentes.

Quelles entités sont concernées par la directive SRI2 ?

Comme précisé plus haut, la directive SRI actuelle s'applique à davantage d'entités que la version précédente. De manière générale, **elle cible principalement les entreprises qui fournissent des services essentiels et importants, en particulier celles avec un effectif d'au moins 50 employés ou un chiffre d'affaires annuel de 10 millions d'euros**.

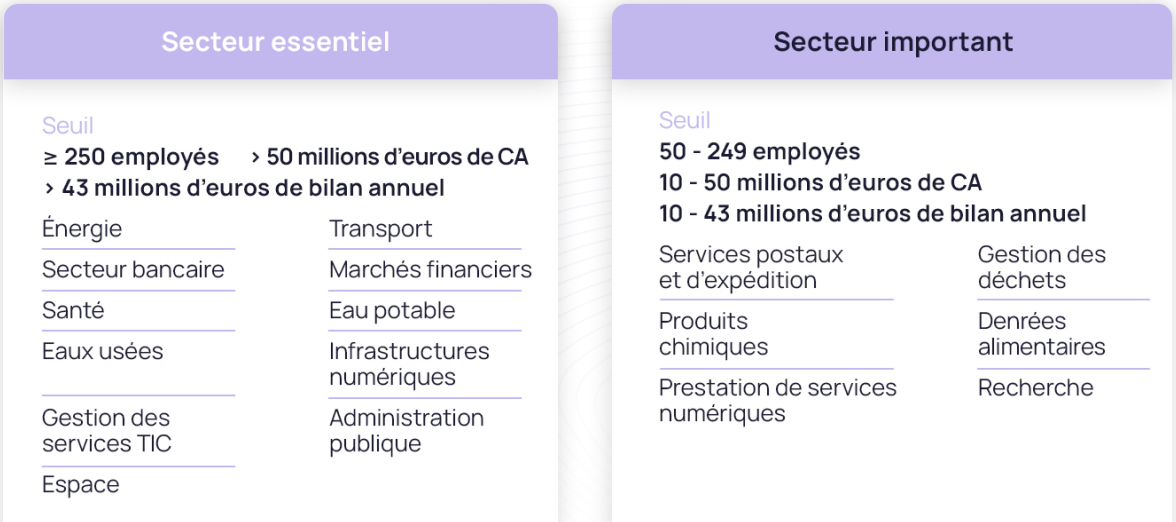
Pour limiter les divergences sur ce qui définit les prestataires de service concernés dans les différents États membres, et donc pour assurer une certaine uniformité, **la directive SRI2 distingue deux groupes d'entités : celles qui sont essentielles et celles qui sont importantes**. Le périmètre d'application est également étendu à d'autres secteurs, fabricants de certains produits ou prestataires de services numériques.

D'après ces nouveaux critères, les **entités essentielles** se définissent comme des organismes comptant au moins 250 employés, avec un chiffre d'affaires annuel de 50 millions d'euros, un bilan annuel de 43 millions d'euros et des activités dans les secteurs de l'énergie, des transports, de la banque, des marchés financiers, de la santé, de l'eau potable, des eaux usées, des infrastructures numériques, de la gestion des services TIC, de l'administration publique et de l'espace. **Les entités importantes** comptent, quant à elles, moins de 250 employés, avec un chiffre d'affaires annuel compris entre 10 et 50 millions d'euros et un bilan annuel inférieur à 43 millions d'euros. Elles opèrent dans les secteurs des services postaux et d'expédition, la gestion des déchets, la fabrication de produits chimiques, de denrées alimentaires et d'autres équipements, la prestation de services numériques et la recherche.

Veuillez noter qu'une société qui dépasse le seuil fixé pour les entités importantes, mais ne remplit pas les critères d'une entité essentielle est tenue de se conformer aux exigences légales applicables aux entités importantes.

Les mêmes mesures de cybersécurité et exigences de signalement s'appliquent aux deux types d'entités, mais les contrôles et les sanctions diffèrent. Les entités essentielles font l'objet de contrôles concernant l'implémentation des mesures, tandis que pour les entités importantes, une enquête ne sera ouverte qu'en cas de non-conformité évidente.

Les structures qui ne répondent pas aux critères établis pour les entités essentielles ou importantes peuvent néanmoins décider de se mettre en conformité avec la directive SRI2 pour améliorer leur système de cybersécurité. Pour s'enregistrer, ces entités devront fournir leur nom, leur adresse, leur numéro d'enregistrement, le secteur dont elles relèvent selon SRI2, l'État membre auquel elles appartiennent, leurs coordonnées et une liste d'adresses IP concernées.



DORA et SRI2 : étude comparative

Pour relever les défis de plus en plus complexes en matière de cyberattaques et préserver les infrastructures numériques et les systèmes essentiels en Europe, la Commission européenne a récemment déployé deux outils législatifs : la directive SRI2 que nous venons de détailler et le règlement DORA (Digital Operational Resilience Act). Les délais prévus pour l'application de ces deux mesures se superposent : le règlement DORA a été initialement proposé en 2020 et finalisé en 2023, tandis que la directive SRI2 a été votée et publiée en 2022 pour une prise d'effet en janvier 2023.

Ces deux textes juridiques poursuivent le même objectif : améliorer la cyberrésilience des sociétés en Europe, mais elles s'appliquent à des secteurs différents. SRI2 élargit le périmètre de la première directive SRI et cherche à harmoniser la cybersécurité et la gouvernance chez les prestataires de services essentiels et importants tels que les transports, les télécoms, la gestion de l'eau et des déchets, les centres de données, le secteur bancaire, l'administration publique, la recherche, les services postaux et d'expédition, etc. De son côté, **DORA est un nouveau règlement visant à préserver l'intégrité des systèmes numériques au sein des entités financières** en Europe et à harmoniser la détection, la gestion et le signalement des risques liés aux TIC.

Bien que leur portée soit différente, la directive SRI2 et le règlement DORA poursuivent un but commun, celui de coordonner les efforts en matière de cybersécurité dans tous les pays européens, de protéger les informations et de limiter les risques de violation dans un contexte où ils ne cessent de se multiplier.

Délai d'application des exigences de la directive SRI2

En juillet 2016, le Parlement européen et le Conseil de l'Union européenne ont adopté la directive SRI pour augmenter le niveau global de cybersécurité dans l'U.E. et renforcer la résilience des infrastructures critiques. Entrée en vigueur en août 2016, elle accordait aux États membres un délai de 21 mois (jusqu'au mois de mai 2018) pour assurer la transposition dans leurs droits nationaux respectifs. Passé cette date, les services essentiels et les prestataires de services numériques devaient être en parfaite conformité avec les réglementations sur la cybersécurité et les obligations de signalement imposées par la directive SRI.

Cependant, face à une transition numérique qui s'accentue et à des cyberattaques récurrentes, le besoin d'une législation plus forte est devenu manifeste en 2020. Il était impératif de protéger les systèmes et les informations des prestataires de services critiques, mais aussi d'élargir la portée de ces mesures à certains secteurs importants. C'est dans cette optique qu'en décembre 2020, la Commission européenne a proposé une version actualisée de la directive SRI, baptisée SRI2. Après une année d'amendements et de négociations, la directive SRI2 a été votée en 2022 et est parue au Journal officiel le 27 décembre 2022.

Officiellement, la directive SRI2 est entrée en vigueur le 16 janvier 2023. Les États membres ont cependant jusqu'au 17 octobre 2024 pour en transposer les mesures dans leur droit national, les rendre publiques et en assurer la conformité. Après cette date, tout manquement aux exigences de SRI2 sera sanctionné par différentes amendes ou taxes pouvant être imposées à des personnes physiques comme aux entités en tant que telles.

Le 17 juillet 2024 et tous les 18 mois par la suite, le réseau EU-CyCLONe devra rédiger un rapport rendant compte de ses travaux. De son côté, le réseau des CSIRT devra également rendre un rapport le 17 janvier 2025. Il y détaillera les progrès réalisés par les États membres en matière de coopération opérationnelle et y formulera ses conclusions et ses recommandations à partir des évaluations par les pairs : efforts en vue de partager des expériences, d'apprendre les uns des autres et de s'entraider pour assurer la conformité de tous. Le 17 avril 2025, les États membres devront dresser une liste des entités essentielles et importantes au sens de SRI2.

La directive SRI2 sera réexaminée en octobre 2027, soit trois ans après son adoption.

Quelles conséquences en cas de non-conformité ?

La directive SRI2 prévoit un certain nombre de sanctions de base en cas d'infractions liées à la gestion des risques de cybersécurité et aux obligations de signalement. Ces pénalités imposées aux structures qui ne respectent pas les délais imposés peuvent se présenter sous des formes variées, notamment des mesures correctives non pécuniaires, des amendes administratives et des sanctions pénales. Le détail de ces sanctions varie cependant selon la structure et les éventuelles divergences entre l'implémentation effective et celle qui est prévue.

Les autorités de contrôle nationales disposent de **voies de droit non monétaires**, notamment d'ordonnances pour exiger la mise en conformité, la réalisation d'audits de sécurité ou la notification des éventuelles menaces aux clients des entités, ainsi que de mesures contraignantes.

Les **amendes administratives** diffèrent selon qu'elles s'appliquent à des entités essentielles ou importantes au sens de la directive SRI2. Pour les entités essentielles, la nouvelle réglementation exige que les autorités nationales imposent une amende maximale d'au moins 10 000 000 € ou de 2 % du chiffre d'affaires annuel mondial selon le chiffre qui est le plus élevé. Pour les entités importantes, l'amende maximale peut être d'au moins 7 000 000 € ou de 1,4 % du chiffre d'affaires annuel mondial selon le chiffre qui est le plus élevé.

Contrairement à la directive précédente, SRI2 transfère la responsabilité de la mise en œuvre et de la maintenance des mesures de cybersécurité du service informatique **aux membres de la direction**. Les États membres peuvent désormais rendre les cadres dirigeants personnellement responsables d'un cyberincident, en cas de négligence grave de la société. Les sanctions qui peuvent s'appliquer dans ce cadre sont notamment : la publication des éventuels manquements aux obligations de conformité, de la nature de ces violations et du nom des personnes physiques et morales qui en sont responsables et, s'il s'agit d'une entité essentielle, l'interdiction, pour ces personnes, d'exercer des fonctions de direction en cas d'infractions répétées.

Prochaines étapes : comment assurer sa conformité à la directive SRI2

Bien qu'un délai généreux de 24 mois soit prévu pour implémenter entièrement la directive SRI2, il est important de s'y préparer suffisamment tôt pour assurer une conformité totale. Il faut du temps pour élaborer une stratégie, coordonner la mise en œuvre avec les prestataires de services tiers et prévoir un budget. Les sociétés ont donc tout intérêt à anticiper sur les mesures à prendre pour que tout soit mis en place à temps et sans stress de dernière minute. Pour bien mettre à profit le délai d'application et assurer leur mise en conformité, les entités peuvent suivre les étapes suivantes :

1. Réunir les instances dirigeantes et les parties prenantes afin de discuter de la stratégie à suivre pour l'implémentation et d'évaluer l'impact de la directive SRI2 sur les activités quotidiennes.

2. S'assurer que tous les membres du conseil d'administration, l'équipe informatique ainsi que les employés responsables des services essentiels comprennent les exigences de la directive SRI2.

3. Dresser la liste des éléments et processus critiques nécessaires à la fourniture des services essentiels et analyser les lacunes afin d'identifier les domaines dans lesquels les mesures de sécurité ne répondent pas aux critères de SRI2.

4. Dresser la liste des prestataires de service tiers qui fournissent des services essentiels, ainsi que de leurs éventuelles vulnérabilités.

5. Élaborer un plan de sensibilisation à la cybersécurité intégrant tous les niveaux hiérarchiques de la société pour que les employés comme la direction soient bien informés des modifications actuelles et futures qui s'appliqueront à leur travail, des attentes en matière de signalement et des autres points de cybersécurité.

6. Trouver des partenaires en matière de conformité à même d'apporter une assistance et des conseils pour assurer la mise en conformité.

7. Prévoir le budget nécessaire pour pouvoir répondre aux exigences de la directive SRI2.

8. Lorsque toutes ces mesures ont été instaurées, procéder à une deuxième évaluation des lacunes pour s'assurer que tout est parfaitement conforme.

Comment SoSafe peut vous aider à assurer votre conformité au règlement SRI2

L'objectif de la directive SRI2 est de compléter et d'améliorer la première directive du nom pour que les prestataires de services essentiels et importants soient en mesure de faire face aux menaces croissantes de cyberattaques. Pour ce faire, les structures doivent adopter une approche holistique qui tient compte des exigences en matière de gestion des risques, des obligations de signalement et des plans de réponse définis dans SRI2.

La nécessité d'une gestion efficace des risques se trouve au cœur de la directive : les articles 7, 9, 20 et 21 soulignent l'importance d'inculquer, tant aux instances dirigeantes qu'au personnel, les connaissances et les compétences suffisantes pour identifier les risques et évaluer les pratiques de cybersécurité.

Dans cette optique, la formation gamifiée de SoSafe peut être d'une aide précieuse, car elle intègre une grande variété de modules couvrant une large gamme de menaces, ainsi que diverses bonnes pratiques pour entraîner vos employés à déceler les menaces et à les combattre efficacement. Le contenu de cette plateforme est disponible dans plus de 30 langues et s'adapte à différents contextes linguistiques, conformément aux exigences en formation dans la langue maternelle qui sont imposées dans plusieurs pays. En outre, la solution Content Management de SoSafe met à la disposition des collaborateurs un service tout-en-un où ils ont accès à tous les modules de formation et aux politiques de sécurité, y compris celles de l'entreprise, afin de stimuler leur engagement et de les aider dans la mise en conformité. Mais la sensibilisation à la cybersécurité va bien au-delà de simples modules de formation : elle doit être intégrée dans la vie et les échanges de tous les jours. Vous pouvez, à cet effet, intégrer notre chatbot, Sofie, dans Microsoft Teams pour communiquer en temps réel avec vos équipes sur les alertes urgentes ou leur envoyer de petits rappels pédagogiques en quelques minutes.

L'article 11 de la directive SRI2 demande aux CSIRT de fournir une analyse dynamique des risques et des incidents, ainsi qu'une sensibilisation à la cybersécurité par le biais de mises en situation. L'outil de pilotage des risques et des alertes de SoSafe est conforme à la norme ISO 27001. Axé sur le facteur humain, il vous permet de suivre les progrès réalisés au niveau des programmes de sensibilisation et d'avoir accès à des analyses, des mesures et des ICP relatifs aux risques humains au sein de votre entreprise. En complément, le bouton d'alerte Phish Assist peut être mis à la disposition des employés pour favoriser un signalement rapide des incidents de sécurité, accélérer la détection des menaces et donner l'alerte le plus tôt possible.

En vous conformant à la directive SRI2 et en instaurant des ressources et une formation adaptées, vous ne ferez pas qu'assurer votre conformité. Vous **renforcerez considérablement les défenses de votre société** contre les menaces cyber, éviterez les interruptions d'activité et contribuerez à la prospérité de votre entreprise.

Établissez une ligne de défense humaine efficace

La plateforme de sensibilisation SoSafe permet aux entreprises de consolider leur culture de la sécurité en limitant les risques humains. Elle propose une expérience d'apprentissage stimulante ainsi que des simulations d'attaques personnalisées qui enseignent aux employés comment protéger activement la société des menaces en ligne. Chaque outil est développé selon les principes des sciences comportementales pour assurer une formation à la fois ludique et efficace. Des analyses détaillées mesurent les fruits de ce programme en matière d'évolution des comportements et révèlent précisément aux sociétés les lacunes à combler pour assurer une réponse proactive face à d'éventuelles menaces. Facile à déployer et évolutive, la plateforme de SoSafe inscrit en chaque employé des réflexes de sécurité, sans lui demander d'efforts démesurés.

ÉDUQUER — Micro-apprentissage stimulant

Une plateforme de formation inspirée des sciences comportementales qui enthousiasme les collaborateurs. Améliorez votre résilience face aux menaces cyber et assurez votre conformité aux obligations légales grâce à une formation dynamique qui joue sur différents canaux pour développer, des réflexes de sécurité qui durent.

- Une pédagogie narrative et gamifiée
- Une bibliothèque de contenus présélectionnés
- Des options de personnalisation et de gestion de contenu qui s'adaptent à chaque entreprise

TRANSMETTRE — Simulations de spear phishing

Des simulations de phishing axées sur l'utilisateur pour développer des réflexes de sécurité. Grâce à nos simulations de spear phishing régulières et automatisées, formez vos employés pour qu'ils sachent détecter les cyberattaques. Vous les aiderez ainsi à adopter des réflexes de sécurité durables dans leurs activités quotidiennes.

- Des simulations de cyberattaques personnalisées et réalistes
- Des explications pédagogiques contextualisées
- Bouton d'alerte phishing qui permet de signaler les menaces en un clic

AGIR —

Suivi stratégique des risques

Protégez votre entreprise contre les incidents et leurs conséquences financières grâce à notre solution d'évaluation du risque humain. Bénéficiez d'un bilan sur l'état de votre couche de sécurité humaine afin de pouvoir anticiper toute vulnérabilité éventuelle. Suivez l'impact de vos programmes, analysez les comportements et prenez des décisions éclairées en matière de protection des données.

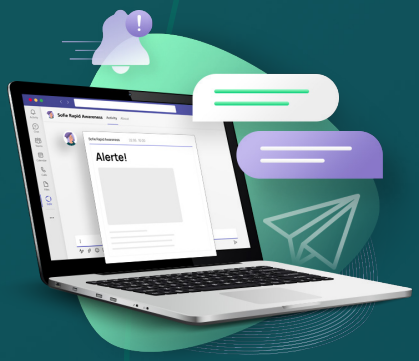
- Des données contextuelles, incluant notamment les ICP techniques et psychologiques
- Des références propres au secteur de l'entreprise et des directives pratiques
- Une solution développée pour répondre aux exigences de la norme ISO/CEI 27001 et conçue selon une approche de « privacy by design »

CONNECTER —

Sofie Rapid Awareness

Les cybercriminels progressent à un rythme effréné… Vous pouvez en faire autant. La formation rapide à la sensibilisation vous permet de vous connecter rapidement avec vos collaborateurs dans MS Teams, pour gérer les menaces qui surgissent avec des micro-apprentissages express, envoyer des alertes en temps réel à votre équipe et leur donner le pouvoir de devenir votre meilleure défense.

- Connexion directe avec votre équipe dans MS Teams
- Gain de temps et facilité de communication
- Envoi de micro-alertes de sécurité faciles à assimiler pour les collaborateurs
- Possibilité de visualiser le nombre de personnes qui ont lu l'alerte pour assurer un maximum de suivi



sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Allemagne

info@sosafe.de
www.sosafe-awareness.com/fr
+49 221 65083800