CHECKLIST POURFACILITER LA MISE EN CONFORMITÉ AVEC LA DIRECTIVE NIS2

Tous les États membres de l'UE vont devoir se conformer à la directive NIS2 d'ici 2024. Cette obligation signifie suivre des stratégies de cybersécurité spécifiques, établir des autorités compétentes et mettre en œuvre des mécanismes de signalement des incidents. La directive NIS2 exige que les États membres de l'UE coopèrent au partage d'informations afin de protéger les actifs vitaux contre les cyberattaques.

Ladirective NIS2 s'appuie sur les exigences de la directive originale : eneffet, elle a toujours pour objectif de protéger les infrastructures et lesorganisations critiques au sein de l'UE contre les cybermenaces et d'atteindreun même niveau élevé de sécurité dans toute l'UE.

Pouratteindre cet objectif, la directive NIS2 exige que les États membres prennentun certain nombre de mesures supplémentaires, notamment :

- Établirun plan de réponse aux incidents coordonné avec les plans des autres Étatsmembres.
- Créer un CERT (Computer Emergency Response Team) national.
- Renforcerla coopération entre les entités des secteurs public et privé.
- Améliorerle partage d'informations entre les États membres.

Pour vous faciliter la tâche, voici une checklist qui va vous aider à vérifier que toutes les conditions sont bien réunies pour vous conformer à la directive NIS2. Il vous suffit de parcourir tout simplement cette liste et de cochez les cases qui correspondent à votre situation. Tout d'abord, pour commencer : la directive NIS2 s'applique-t-elle à votre organisation ? Probablement que oui !

Travaillez-vous dans l'un de ces secteurs ?

☐ Énergie	☐ Banque	☐ Espace
☐ Gouvernement	☐ Finance	☐ Services postaux et de messagerie
☐ Administration publique	☐ Secteur manufacturier	☐ Gestion globale des déchets
☐ Transport	☐ Eau (déchets/potable)	☐ Produits chimiques (élimination/production)
☐ Forces de l'ordre	☐ Infrastructures numériques	☐ Science
☐ Éducation	☐ Secteur de la santé	☐ Industrie alimentaire

La conformité avec la directive NIS2 n'est pas une option. Pour ce faire, vous devez répondre à un ensemble d'exigences, mais toute démarche de mise en conformité commence par la mise en place des fondamentaux avant même d'arriver aux solutions et autres plateformes de sécurité. Vous devez vous assurer que vos collègues au sein de l'entreprise ou de l'organisation soient bien conscients de leurs propres responsabilités dans ce processus. Cette garantie permettra de minimiser les risques, et ce dès le départ.

Important à noter : la gestion et l'évaluation des risques est unprocessus continu. Il se déroule suivant un protocole bien précis. Une foisl'évaluation des risques effectuée, il est important de planifier des mises àjour régulières pour garantir que toutes les étapes soient correctementexécutées.

Considérez les phasessuivantes comme des étapes à part entière : 1. Sensibilisation. 2. Sécurité RH. 3. Contrôle desactifs : où se trouvent-ils, combien en possédez-vous, sont-ils tous àjour ? 4. Gestion des incidents de manière standardisée et cohérente. 5.Gestion des vulnérabilités : vos systèmes sont-ils à jour ? 6. Évaluationdes risques au niveau de la supply chain. 7. Sécurité du réseau. 8. Sécurité desprocessus de développement : savez-vous qui a écrit votre code, êtes-voussûr que personne d'autre n'a pu créer des backdoors ? 8. Contrôle d'accès, à lafois physique et virtuel. 9. Utilisation du chiffrement le cas échéant. 10.Plan d'urgence : que faites-vous si un individu compromet votre réseau, volevos données ou bien si vous êtes victime d'un ransomware ?

MAINTENANT NOUS POUVONS ENTRER DANS LES DÉTAILS

Pour vous :

- [ ] Avez-vous pris connaissance des exigences de la directive NIS2 ?
- [ ] Comprenez-vous bien la différence essentielle entre les directives NIS et NIS2 ?
- [ ] Savez-vous qui est en charge de la conformité et qui est tenu responsable si vous ne vous conformez pas ?
  - [ ] Très important : les personnes concernées savent-elles qu'elles sont responsables/impliquées ?
- [ ] Votre infrastructure dispose-t-elle de capacités de réponse aux incidents et de gestion de crise ?
- [ ] Comment allez-vous gérer les vulnérabilités et la divulgation ?
  - [ ] Avez-vous procédé à une évaluation des risques liés à un tel cas de figure ?
- [ ] Évaluation de votre supply chain : est-elle sécurisée ?
  - [ ] Avez-vous évalué les risques potentiels au niveau de votre supply chain ?
  - [ ] Avez-vous évalué les risques associés à vos clients ?

Pour que vous puissiez aider vos collègues :

- [ ] Avez-vous mis en place des politiques et des procédures pour évaluer votre cybersécurité ?
- [ ] Avez-vous suivi une formation en cybersécurité ?
- [ ] Avez-vous sensibilisé vos collègues à l'importance de la gestion et conformité des données ?
- [ ] Avez-vous effectué une évaluation de la maturité de votre organisation ?
- [ ] Avez-vous un plan précis à mettre en œuvre pour élaborer une stratégie ?

Hygiène IT

Il est essentiel d'informer les membres de votre organisation de la nécessité de se conformer aux normes telles que le RGPD et le NIS2. La manière avec laquelle ces derniers gèrent les données de manière concrète, à savoir sur le terrain, peut avoir un impact considérable sur les données elles-mêmes et la conformité en général. S'ils ne savent pas comment ils doivent gérer les données et les informations, ou bien s'ils pensent qu'ils le font correctement, et que ce n'est pas le cas en réalité : alors vous êtes face à un vrai problème.

- ☐ Avez-vousévalué vos pratiques de base en matière d'hygiène IT ?
  - ☐ Sont-elles suffisantes pour se conformer à ladirective NIS2 ?
- ☐ Avez-vousune politique d'hygiène en matière de cybersécurité ?
  - ☐ Si non, allez-vous créer une telle politique ?
  - ☐ Avez-vous largement diffusé cette politique au seinde toute l'entreprise et même au niveau de l'équipe dirigeante ?
- ☐ Disposez-vousd'une plateforme de sécurité centrale ?
  - ☐ Pouvez-vous automatiser les tâches courantes ?
- ☐ Avez-vousmis en place des politiques strictes en matière de mots de passe pourl'ensemble du personnel ?
- ☐ Vousêtes-vous assuré d'avoir mis en place une authentification multifacteursuffisante ?
- ☐ Avez-vousmis en place une protection endpoint ?
- ☐ Avez-vousdéployé des frameworks adaptés : NIST /ISO/CIS/ MITRE ATT&CK ?

Cryptographie

- ☐ Disposez-vous des supports nécessaires pour expliquer la cryptographie à ceux qui en ont besoin ?
- ☐ Avez-vous utilisé la cryptographie de manière efficace ?

Divers/Autres

- ☐ Avez-vousdes pratiques RH conformes en matière de cybersécurité ?
- ☐ Avez-vousmis en place des politiques de sécurité au niveau des ressources humaines enmatière d'accès et de contrôle ?
- ☐ Avez-vous évalué les risques liés à vos politiquesd'accès et de contrôle en matière de sécurité RH ?

Non-conformité

- ☐ Êtes-vous conscient des conséquences en cas de non-conformité ?

Comment une plateforme de cybersécurité efficace peut vous aider à garantir votre conformité ?

- ☐ Avez-vous mis en place des mesures de cybersécurité suffisantes ?
  - ☐ SIEM ☐ SOAR ☐ UEBA ☐ Sécurité du système et des applications SAP ☐ Sécurité endpoint
  - ☐ S'agit-il d'une solution Saas ?
  - ☐ S'agit-il d'une solution Saas avec stockage physique des données dans l'UE ?

Reporting

Les signalements sont une exigence de la directive NIS2 :

24h : alerte précoce indiquant si l'incident a été causé par une action illégale ou malveillante ou bien si elle pourrait avoir un impact externe.

72h : notification comprenant une évaluation initiale avec la gravité, l'impact et l'IoC. Rapports immédiats concernant l'évolution de la situation (mise à jour de statut) conformément aux exigences des autorités.

En plus : un rapport final au plus tard un mois après la première notification qui comprend une description détaillée des incidents, les types de menace, les mesures de mitigation et l'impact externe des incidents.

☐ Votre plateforme de sécurité vous fournit-elle des playbooks qui rassemblent, convertissent et diffusent automatiquement les informations pour se conformer aux exigences en matière de reporting ?

Gestion des incidents

☐ La directive NIS2 définit la gestion des incidents comme suit : toutes les actions et procédures visant à prévenir, détecter, analyser, contenir ou répondre et enfin à récupérer les systèmes après un incident.

☐ Disposez-vous d'une solution consolidée qui facilite la gestion des incidents ?

☐ Disposez-vous d'une sécurité SAP en place/capacité à signaler les problèmes SAP/visibilité sur les systèmes SAP pour la surveillance et la gestion des incidents ?

Certification et conformité additionnelles

☐ Votre sécurité est-elle certifiée Common Criteria EAL3+ ?
☐ Est-elle conforme à la norme ISO 15408 ?
☐ Votre cybersécurité est-elle conforme à :
  ☐ GDPR
  ☐ Schrems II
  ☐ CCPA

POUR EN SAVOIR PLUS

À PROPOS DE LOGPOINT

Logpoint est le créateur d'une plateforme d'opérations de cybersécurité fiable et innovante, permettant aux entreprises du monde entier d'évoluer et se développer dans un monde constitué de menaces en constante évolution. En combinant une technologie sophistiquée et une compréhension approfondie des défis de ses clients, Logpoint renforce les capacités des équipes de sécurité tout en les aidant à lutter contre les menaces actuelles et futures. Logpoint propose les technologies de sécurité SIEM, UEBA, SOAR et SAP convergées dans une plateforme complète qui détecte efficacement les menaces, minimise les faux positifs, priorise les risques de manière autonome, répond aux incidents et bien plus encore. Basée à Copenhague, au Danemark, et possédant des bureaux dans le monde entier, Logpoint est une entreprise multinationale, multiculturelle et inclusive.