kaspersky bring on the future

Directive NIS 2 de l'UE : nouvelles obligations et ce que vous pouvez faire pour vous y préparer

Quel est l'objet de la directive NIS 2 ?

La directive NIS 2[1] est entrée en vigueur le 16 janvier 2023, et les États membres devront la transposer d'ici le 17 octobre 2024. Outre d'autres objectifs, la directive NIS 2 impose aux principaux opérateurs des industries clés de prendre des mesures de sécurité et de signaler les incidents.

À qui s'applique la directive NIS 2 ?

Une entité est visée par le champ d'application de la directive dès lors qu'elle opère dans l'un des secteurs et types de services énumérés dans les annexes de la directive et qu'elle atteint une certaine taille. Pour connaître tous les détails, toutes les exceptions et toutes les nuances, il convient de se référer aux articles 2 et 3 et aux annexes I et II de la directive[2]. La directive NIS 2 établit deux catégories d'entités qui entrent dans son champ d'application, à savoir les entités essentielles et les entités importantes. Ces deux catégories doivent satisfaire aux mêmes exigences. La distinction entre les deux catégories réside dans les mesures de contrôle et les sanctions.

Quelles sont les exigences de la directive NIS 2 en matière de cybersécurité ?

Conformément à l'article 21-1 de la directive, les États membres doivent veiller à ce que les entités essentielles et importantes prennent des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information que lesdites entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, et pour prévenir ou réduire au maximum l'impact des incidents sur les bénéficiaires de leurs services et sur d'autres services.

Ces mesures doivent être fondées sur une approche tous risques qui vise à protéger les réseaux et les systèmes d'information ainsi que l'environnement physique de ces systèmes contre les incidents, et doivent comprendre au moins les éléments suivants :

- Politiques en matière d'analyse des risques et de sécurité des systèmes d'information ;
- Traitement des incidents :
- Continuité des activités, comme la gestion des sauvegardes et la reprise après sinistre, ainsi que gestion des crises ;
- Sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité des relations entre chaque entité et ses fournisseurs directs ou ses prestataires de services ;
- Sécurité dans l'acquisition, le développement et la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
- Politiques et procédures visant à évaluer l'efficacité des mesures de gestion des risques liés à la cybersécurité ;
- Pratiques de base en matière de cyberhygiène et formation à la cybersécurité ;
- Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
- Sécurité des ressources humaines, politiques de contrôle d'accès et gestion des ressources ; utilisation de solutions d'authentification multifacteur ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes de communication d'urgence sécurisés au sein de l'entité, le cas échéant.

[1] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 relative à des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive NIS 2) ; https://eur-lex.europa.eu/eli/dir/2022/2555
[2] https://eur-lex.europa.eu/eli/dir/2022/2555

Quelles sont les sanctions en cas de non-conformité ?

Les autorités compétentes peuvent infliger des amendes administratives importantes en cas de violation des obligations prévues par la législation nationale transposant la directive NIS 2. Ces amendes peuvent atteindre un maximum de 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial du groupe dans le cas d'entreprises ou d'entités essentielles, ou de 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial du groupe dans le cas d'entreprises ou d'entités importantes.

Comment les entreprises devraient-elles se préparer ? Recommandations

Les entreprises et autres entités devraient commencer à se préparer dès à présent :

- En déterminant si et dans quelle mesure elles seront soumises aux obligations en matière de cybersécurité prévues par la directive NIS 2.
- En vérifiant la transposition de la directive NIS dans le droit national de leur État membre.
- En suivant les informations et les recommandations données par les autorités nationales chargées de la cybersécurité[3].
- En évaluant et en développant leurs mesures techniques, opérationnelles et organisationnelles pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information.

Comment les solutions et les prestations de Kaspersky peuvent-elles aider votre entreprise ?

En tant que fournisseur de cybersécurité, Kaspersky met à profit toute son expertise pour aider les entreprises à mettre en place des cyberdéfenses fiables. Nous pouvons vous aider grâce aux solutions et services suivants :

Endpoint Detection and Response (EDR) est une solution technique qui fournit des informations approfondies relatives à ce qui se passe sur vos terminaux. Avec Kaspersky Endpoint Detection & Response (EDR) Optimum, vous pouvez analyser de manière proactive votre serveur et votre réseau de clients à la recherche d'indicateurs de compromission (IoC) spécifiques. Votre service informatique ou un fournisseur de services externe acquiert ainsi une connaissance approfondie des cyberattaques imminentes et peut, le cas échéant, prendre des mesures immédiates (). En cas d'incident, vous recevez des données importantes destinées à l'analyse des causes profondes.

Managed Detection and Response (MDR) vous permet d'externaliser votre cyberprotection en la confiant à nos experts expérimentés. Les chercheurs de menaces de Kaspersky surveillent les données télémétriques de vos systèmes informatiques et détectent immédiatement toute activité suspecte. Ce service, disponible 24 heures sur 24 et 7 jours sur 7, est assuré par des spécialistes répartis dans différents centres d'opérations de sécurité (SOC) à travers le monde.

Formation de sensibilisation : Kaspersky a mis au point un concept global efficace pour développer l'expertise d'une entreprise en matière de cybersécurité. Notre offre va de la formation générale pour sensibiliser et motiver votre équipe, à la formation spécialisée pour le personnel du service d'assistance, en passant par la formation en ligne pour les responsables. Notre plateforme de formation interactive en ligne, KASAP, propose une formation pratique de sensibilisation à la sécurité pour votre équipe, qui peut être facilement intégrée à leur routine de travail quotidienne. Les participants peuvent suivre les modules d'apprentissage en ligne de manière flexible et les reprendre à tout moment.

Threat Intelligence (TI) : Notre Threat Intelligence (TI) de pointe offre aux entreprises une vision à 360 degrés du paysage des menaces. Elle leur donne accès à la base de données complète de Kaspersky sur les menaces et à une connaissance approfondie de l'environnement informatique et technologique. Cela leur permet de détecter rapidement les attaques imminentes, de renforcer leurs mesures de sécurité et d'endurcir leurs systèmes.

Réponse aux incidents (RI) : En cas d'incident de sécurité, les entreprises bien préparées ont l'avantage de pouvoir réagir plus rapidement et plus efficacement. Kaspersky propose une gamme de services de réponse aux incidents pour aider les entreprises à se préparer à une situation d'urgence. Par exemple, Kaspersky Tabletop Exercise (TTX) est un exercice guidé qui vous permet de revoir vos processus et plans de réponse aux incidents. Vous identifierez les lacunes de votre plan d'urgence, vous clarifierez les rôles et les responsabilités de vos équipes, et vous améliorerez la coordination entre vos différents services.

Cybersécurité industrielle : Kaspersky Industrial Cybersecurity (KICS) est une solution industrielle éprouvée et certifiée qui répond aux besoins spécifiques des entreprises industrielles et des opérateurs d'infrastructures critiques en matière de cybersécurité. KICS protège déjà plus de 1 000 clients industriels de premier plan à travers le monde.

Kaspersky comprend les besoins des différentes industries et des différentes tailles d'entreprises et **protège plus de 220 000 entreprises à travers le monde** contre les cybermenaces.
La cyberprotection fiable et tout-en-un de Kaspersky couvre de multiples aspects en matière de protection.

Protégez-vous dès maintenant !

[3] Voir par exemple les recommandations du NCSC d'Irlande : https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf ; de l'ANSSI française : https://www.ssi.gouv.fr/directive-nis-2/ ; ou du CCBde Belgique : https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization#_Toc128118851

Nouvelles sur les cybermenaces : securelist.com/
Blog de Kaspersky : kaspersky.fr/blog
Cybersécurité pour les grandes entreprises : kaspersky.fr/enterprise-security
Cybersécurité pour les entreprises de taille moyenne : kaspersky.fr/small-to-medium-business-security

kaspersky.fr