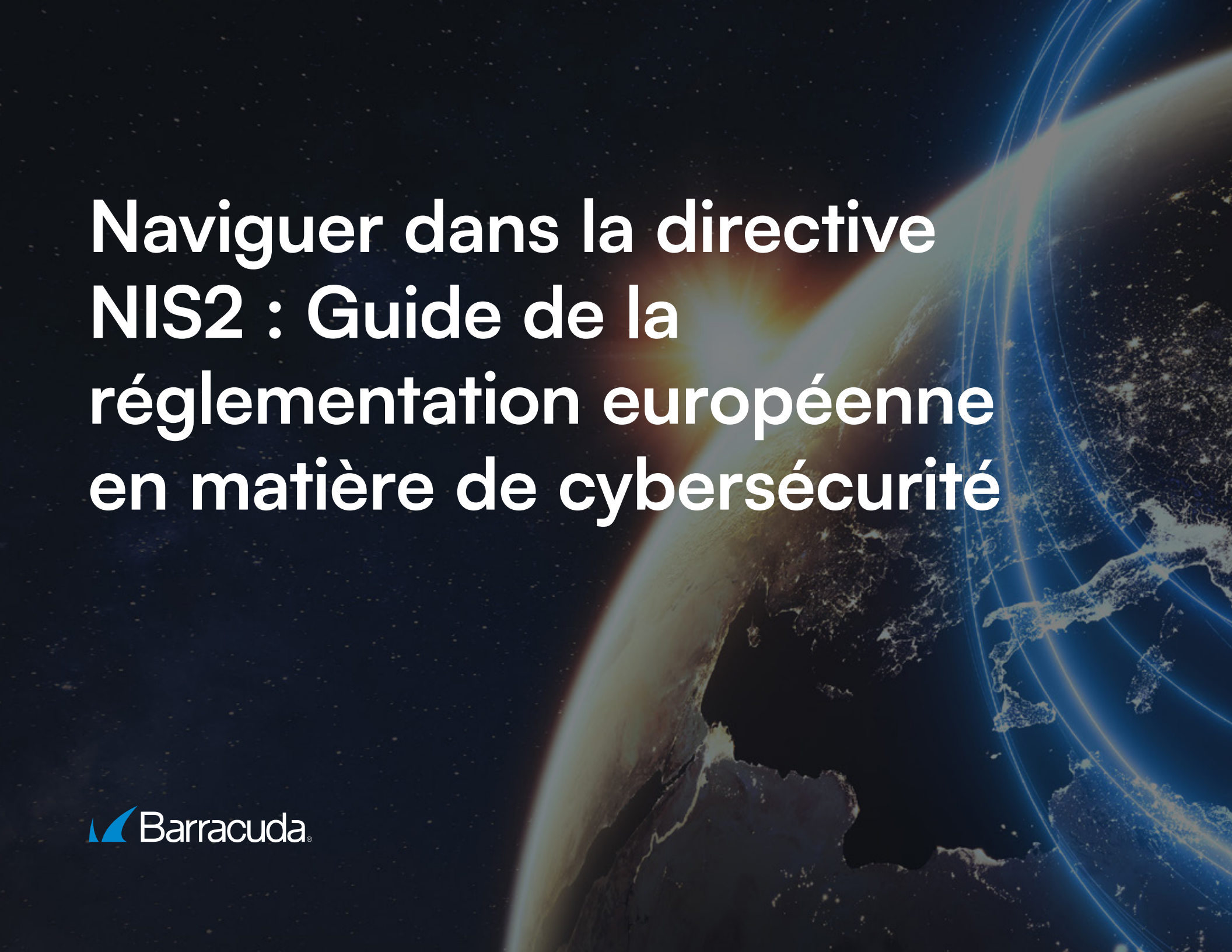
Naviguer dans la directive NIS2 : Guide de la réglementation européenne en matière de cybersécurité



Barracuda

L'évolution des réglementations en matière de cybersécurité en Europe

L'évolution du rôle des réglementations en matière de cybersécurité en Europe reflète la reconnaissance croissante de la menace grandissante que les violations et les cybercriminels font peser sur les entreprises, les organisations et la société dans son ensemble. En effet, notre société étant désormais composée d'organisations de plus en plus interconnectées, toute attaque peut avoir des conséquences inattendues et de grande ampleur.

Les modifications récentes apportées à la réglementation de l'Union européenne (UE), connues sous le nom de NIS2 (Directive sur la sécurité des réseaux et de l'information 2), mentionnent également l'impact de la pandémie de COVID-19 sur les pratiques de travail. Comme nous sommes de plus en plus nombreux à travailler à domicile depuis la pandémie, la surface de menace potentielle augmente, tout comme notre dépendance aux réseaux pour accomplir notre travail et mener à bien le reste de notre vie.

Cependant, cela reflète également la maturité croissante de la réglementation en matière de cybersécurité. Bien que les organisations s'efforcent de maintenir leur sécurité, nous savons également que des lois unifiées et des normes minimales sont nécessaires pour assurer notre sécurité à tous.

La première étape de ce parcours a été franchie en 2016, avec la directive sur la sécurité des réseaux et de l'information (NIS1). Cette directive a établi des normes de base en matière de cybersécurité pour les organisations travaillant dans des secteurs critiques tels que l'eau, les infrastructures numériques, les banques, les soins de santé et les transports. La directive NIS2 développe ces normes en englobant un nombre beaucoup plus important de secteurs.

Il convient de noter que la NIS2 est une directive et non une loi. Elle doit donc être transposée en droit national par les États membres, ce que certains ont déjà fait. La NIS2 est désormais en vigueur et plusieurs pays, dont la Belgique, la Croatie et l'Italie, l'ont intégrée dans leur législation locale, tandis que d'autres sont en train de l'adopter.

La directive NIS2 transforme et documente la réglementation au sein de l'UE et au-delà. C'est là un autre élément clé de la législation sur la cybersécurité. La cybersécurité n'est pas l'apanage d'un seul État-nation. Les entreprises qui interagissent avec des citoyens ou d'autres entreprises dans l'UE doivent suivre les mêmes règles. Nous nous dirigeons vers un monde où les normes de cybersécurité sont partagées entre les pays, et les entreprises devront s'y conformer pour faire des affaires et rassurer leurs clients sur la mise en œuvre des réglementations.

Il convient également de noter que le gouvernement britannique s'est engagé à ne pas intégrer la NIS2 dans la législation nationale, mais à étendre la NIS1 conformément à d'autres réglementations, telles que le projet de loi sur la cybersécurité et la résilience (Cyber Security and Resilience Bill). Toutefois, si l'on se penche sur ces déclarations, il semble que le Royaume-Uni et l'UE évoluent dans la même direction en ce qui concerne les modifications en cours, même si la législation britannique proposée promet d'être moins contraignante. On ignore également quand le gouvernement trouvera le temps parlementaire nécessaire pour procéder à ces changements. En réalité, la plupart des organisations qui travaillent ou font du commerce avec l'UE choisiront probablement de se conformer à un seul ensemble de règles plutôt qu'aux deux.

Les bases de NIS2

Qui ?

Cela s'applique à l'ensemble de l'UE, mais les entreprises du monde entier qui font des affaires avec des entreprises ou des organisations de l'UE, ou qui leur fournissent des services, devront également se conformer aux pratiques de la NIS2.

Étend les règles applicables aux grandes organisations gérant des infrastructures critiques aux petites entreprises et à celles qui sont définies par l'UE comme essentielles.

Dans certains secteurs, les règles sont étendues aux entreprises de plus de 50 employés.

Sont concernés les secteurs de l'énergie, des transports, des banques, de la santé, des infrastructures numériques, des fournisseurs de cloud computing, des fournisseurs de services de sécurité gérés, de la gestion des déchets, des producteurs alimentaires, de grandes parties de l'industrie manufacturière, des moteurs de recherche et des organismes de recherche.

Événement :

Établit des règles pour que les pays soient préparés aux incidents de cybersécurité et encourage la coopération transfrontalière.

Les États membres étaient censés transposer la directive en droit national avant octobre 2024. Plusieurs l'ont fait, tandis que d'autres en sont à divers stades d'adoption. Consultez l'état actuel de la transposition.

Notification obligatoire des incidents.

Comment ?

La cybersécurité relève clairement de la responsabilité de la haute direction, et la directive NIS2 le confirme en les tenant personnellement responsables des défaillances.

La directive, et ses équivalents en droit national, couvre un plus grand nombre d'entreprises et d'organisations. Il ne s'agit plus seulement d'infrastructures vitales, mais aussi de celles définies par l'UE comme essentielles.

Définit l'obligation de donner un avertissement précoce des incidents dans les 24 heures, de fournir une notification plus détaillée dans les 72 heures et un rapport détaillé dans le délai d'un mois. Cette mesure vise à produire deux effets positifs : d'une part, encourager le respect des règles sous la menace d'une publicité négative et, d'autre part, fournir des informations exploitables à d'autres organisations susceptibles d'être la cible d'attaques similaires.

Les bases de la NIS2 : Ce que vous devez faire pour vous y conformer

Il faut souligner que la directive NIS2 ressemble fort à un manuel de « bonnes pratiques » pour une hygiène générale en matière de cybersécurité, bien qu'elle soit assortie de lourdes sanctions financières en cas d'échec. Les sanctions prévues par la directive NIS2 sont sévères, avec des amendes pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

La conformité avec la directive et la protection de l'entreprise impliquent de déterminer ce qui est nécessaire pour protéger les appareils, les actifs et les données. Cela suppose une sécurité physique, une cybersécurité et un personnel formé pour agir en toute sécurité. Outre la mise en œuvre de ces mesures, les organisations doivent également justifier de la présence d'une stratégie efficace de gestion des risques. Cela implique de prouver ce que vous avez accompli, à savoir que vous avez évalué l'état de vos réseaux, de vos systèmes informatiques et de vos compétences humaines, et que vous avez pris les mesures adéquates.

Vous devez montrer que vous avez mis en place un plan de gestion des incidents si le pire venait à se produire. Vous devez démontrer que vous avez évalué la sécurité de la chaîne d'approvisionnement, le traitement et la divulgation des vulnérabilités, et que vous avez mis en place une stratégie pour l'utilisation de la cryptographie et, le cas échéant, du chiffrement.

La NIS2 prend en compte les certifications européennes de produits et de solutions en matière de cybersécurité afin d'alléger la charge de conformité pour les entreprises. Si votre organisation est déjà conforme à la norme ISO 27001, vous êtes sur la bonne voie pour satisfaire aux exigences de la NIS2.

Mais, comme toujours, la conformité ne doit pas être considérée comme une fin en soi. Elle peut constituer un excellent moyen de séduire le public et d'obtenir un soutien général pour les stratégies de cybersécurité, qui devraient de toute façon faire partie de la réflexion des entreprises à tous les niveaux. Si la conformité n'est pas synonyme de protection totale, elle ne vous exposera certainement pas à davantage de risques.

La plupart des organisations comprennent désormais qu'elles doivent se préparer aux incidents, tout en espérant qu'ils ne se produisent jamais et en œuvrant activement pour les éviter.

Parallèlement, l'état d'esprit a changé en ce qui concerne le signalement des incidents. Un plus grand nombre de personnes reconnaissent désormais les avantages et le rôle que joue le signalement d'incidents dans la protection d'autres organisations, et comprennent qu'il fournit un plan de défense contre de nouvelles attaques.

Bonnes pratiques en matière de conformité et de sécurité : Comprendre la différence

Les professionnels de la cybersécurité doivent comprendre la différence entre la conformité et la meilleure protection possible. Ces deux notions sont bien différentes. Les organisations doivent justifier de leur conformité ; elles doivent être en mesure de montrer, preuves à l'appui, à un tiers que ce qu'elles ont fait est aussi sûr que possible. C'est comme si vous deviez montrer à votre compagnie d'assurance que vous avez mis en place des serrures et des alarmes adaptées pour protéger votre entrepôt. Tout cela est nécessaire, mais vous devez aller encore plus loin pour être vraiment en sécurité.

Voici 13 éléments à prendre en compte dans votre parcours vers la conformité NIS2 :

Politique de sécurité du réseau : Établissez une politique de sécurité des réseaux et des systèmes d'information qui définit les rôles et les responsabilités des différents services de l'entreprise, ainsi qu'un processus de contrôle de la conformité.

Évaluation des risques : Établissez et mettez en œuvre une politique de gestion des incidents définissant les rôles, les responsabilités et les procédures de détection, d'analyse, de confinement ou de réponse, de récupération, de documentation et de notification des incidents en temps opportun.

Continuité des activités et gestion de crise : Élaborez et tenez à jour un plan de continuité des activités, de gestion de crise et de reprise après sinistre à appliquer en cas d'incidents de cybersécurité et d'autres crises, qui prévoit des plans de secours pour les ressources essentielles, y compris le personnel. Formez le personnel concerné sur ces documents et effectuez régulièrement des simulations de crise pour vous assurer que tout le monde connaît et peut jouer son rôle.

Politique de sécurité de la chaîne d'approvisionnement : Créez et mettez en œuvre une politique de sécurité de la chaîne d'approvisionnement qui comprend une évaluation des pratiques de sécurité des fournisseurs potentiels dans le cadre du processus de passation des marchés.

Comprendre l'utilisation des fournisseurs de technologies de l'information et de la communication (TIC) : Répertoriez vos fournisseurs de TIC, leurs activités, ceux qui sont essentiels à vos opérations et les normes de sécurité qu'ils doivent respecter. Tenez un registre de vos fournisseurs essentiels, avec leurs coordonnées. Mettez en place un processus pour évaluer la conformité des fournisseurs avec les normes de sécurité.

Évaluation des processus de gestion des cyber-risques : Créez un processus permettant d'évaluer l'efficacité de vos procédures de gestion des risques cyber et effectuez cette évaluation périodiquement.

Formation à la sécurité : Dispensez une formation à la cybersécurité et encouragez votre personnel à adopter des pratiques d'hygiène cyber de base afin de promouvoir une culture de sensibilisation à la sécurité.

Cryptographie : Développez et appliquez l'utilisation adéquate de la cryptographie et du chiffrement pour garantir la confidentialité et l'intégrité des données sensibles.

Sécurité des RH : Mettez en œuvre des politiques et des procédures qui régissent le comportement des employés en matière d'hygiène de cybersécurité. Utilisez des procédures de vérification des antécédents appropriées en conformité avec la loi applicable lors de l'embauche de personnel. Créez un processus standard pour révoquer tout accès aux actifs de technologie de l'information de l'entreprise et aux informations de l'entreprise lorsque les employés quittent l'entreprise.

Contrôle des accès : Mettez en place des procédures de sécurité pour les employés ayant accès aux données confidentielles. Utilisez l'authentification multifacteur (MFA) et l'évaluation continue Zero Trust et, le cas échéant, chiffrez les communications d'urgence internes pour renforcer les mesures de sécurité.

Classifier les actifs de l'entreprise : Mettez en place un système pour classer les informations de l'entreprise, telles que les informations confidentielles et les informations sensibles (par exemple, les informations de santé, les numéros d'identification nationaux, les cartes bancaires, etc.).

Sécurité environnementale et physique : Évaluez les infrastructures essentielles de soutien pour les sites de l'entreprise, telles que les systèmes de communication et l'alimentation, et, si possible, mettez en place des processus de sauvegarde. Protégez les emplacements physiques contre les menaces extérieures, y compris les contrôles d'accès physiques.

Les personnes et les processus d'abord, la technologie ensuite

Les fournisseurs sont souvent coupables de vendre d'abord des solutions. Mais en réalité, il faut commencer par mettre en place les bons processus, les bonnes procédures et les bonnes personnes, puis penser à la technologie pour soutenir et renforcer ces capacités. Les équipes de sécurité perçoivent souvent les humains comme le maillon faible plutôt que comme leur première ligne de défense.

La formation de votre personnel et l'amélioration de ses compétences en matière de sécurité constituent une étape essentielle, confirmée par la directive NIS2.

Tout changement de réglementation est une opportunité de repenser les bases et d'évaluer les points forts et les points à améliorer.

Il vous faut de bons contrôles d'accès et une bonne gestion des identités. Vous devez protéger votre messagerie électronique, qui reste le vecteur et le point de départ le plus courant des attaques. Vous avez également besoin d'une protection réseau et de firewalls.

Mais vous avez également besoin de systèmes de sécurité plus intelligents qui travaillent pour vous. Analyser le comportement du réseau et des applications est de plus en plus important dans un monde où l'identification de la « périphérie » d'un réseau est chaque jour plus difficile. Cela peut également vous aider à vous protéger contre les attaques de la chaîne d'approvisionnement.

Barracuda peut vous aider à répondre aux exigences de la NIS2 et à renforcer votre posture de sécurité globale avec une protection des applications, une protection du réseau et des e-mails. Nous pouvons même fournir une solution XDR gérée pour superviser le tout.

Barracuda en quelques mots

Barracuda est une entreprise de cybersécurité leader sur son marché, offrant aux entreprises de toutes tailles une protection complète face aux menaces complexes. Notre plateforme BarracudaONE, propulsée par l'IA, sécurise les emails, les données, les applications et les réseaux grâce à des solutions innovantes, un XDR managé et un tableau de bord centralisé afin de maximiser la protection et renforcer la résilience cyber. Des centaines de milliers d'organisations et de fournisseurs de services managés (MSP) du monde entier nous font confiance pour les protéger et les accompagner, avec des solutions faciles à acquérir, déployer et utiliser. Pour plus d'informations, visitez fr.barracuda.com.

Barracuda