Appréhender la directive NIS2 : un guide sur les futures réglementations européennes en matière de cybersécurité

Barracuda

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 hackers font peser sur les entreprises, les organisations et la société dans son ensemble. Cette dernière étant désormais composée d'organisations de plus en plus interconnectées, toute attaque peut avoir des conséquences inattendues et de grande ampleur.

Les derniers changements apportés à la réglementation de l'Union européenne (UE), appelée NIS2, évoquent également l'impact de la COVID-19 sur les pratiques de travail. Comme nous sommes de plus en plus nombreux à travailler à distance, la surface de menace potentielle augmente, tout comme notre dépendance à l'égard des réseaux pour mener à bien notre travail (et nos autres activités).

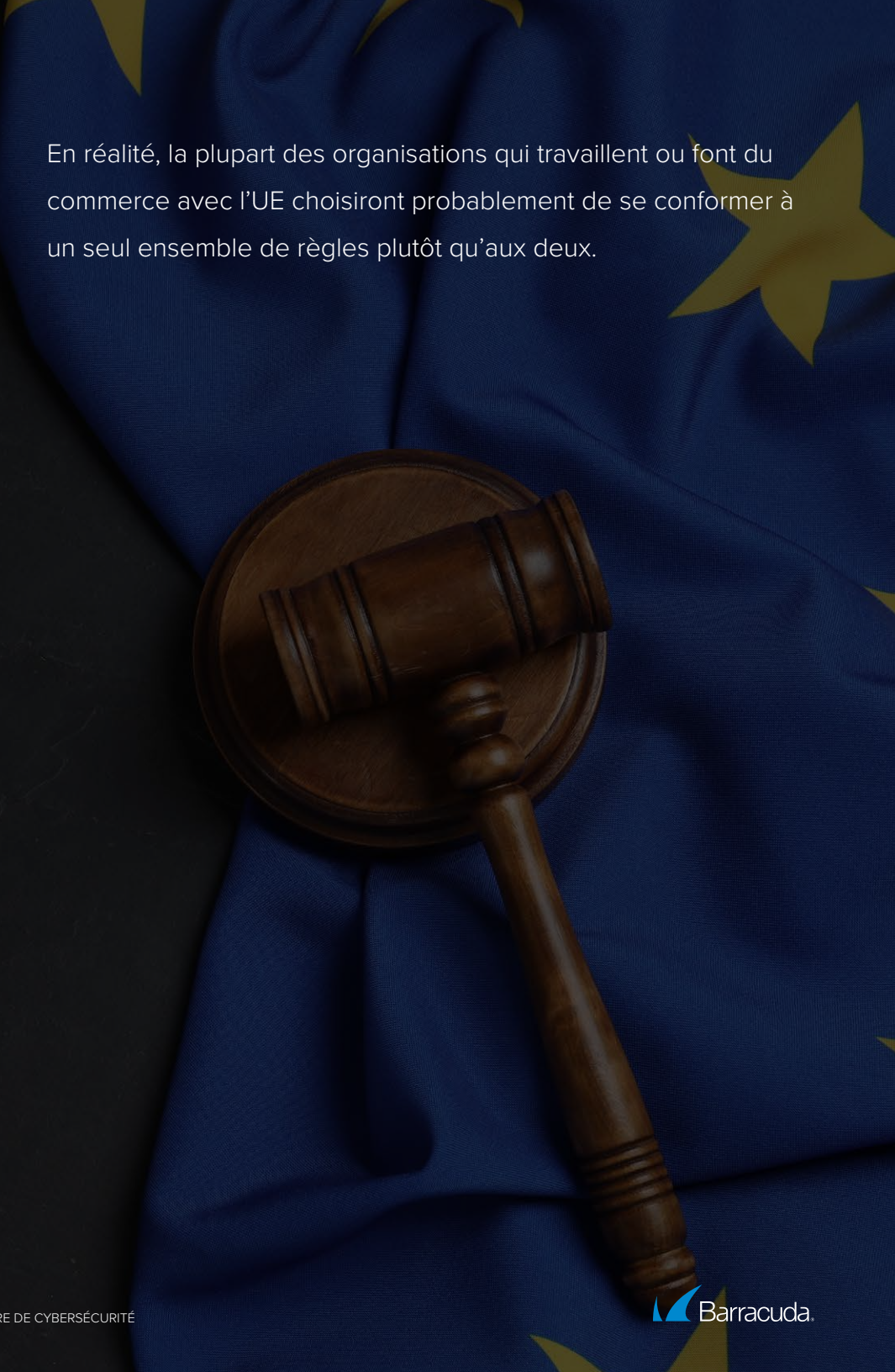
Cependant, cela reflète également la maturité croissante de la réglementation en matière de cybersécurité. Il ne suffit plus d'espérer que les entreprises et les organismes du secteur public redoublent d'efforts pour se protéger. Nous savons désormais que des lois unifiées et des normes minimales sont 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 (Network and Information Security Directive, ou NIS1). Cette directive établit 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 toutefois de noter que la NIS2 est une directive et non une loi ; elle doit être transposée en droit national par les États membres, probablement d'ici l'automne 2024. Mais même avant qu'elle ne soit juridiquement contraignante, les grandes lignes de la directive sont susceptibles de guider la réglementation au sein et en dehors de l'UE pour les années à venir. 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 devront suivre les mêmes règles. Nous nous dirigeons vers un monde où les normes de cybersécurité sont communes à tous les pays, et les entreprises seront tenues de s'y conformer pour exercer leurs activités et rassurer leurs clients.

Il convient également de noter que le gouvernement britannique s'est engagé à ne pas adopter la NIS2 dans sa législation nationale, mais à étendre la NIS1. Toutefois, si l'on se penche sur les propositions actuelles, le Royaume-Uni et l'Union européenne semblent aller dans la même direction, même si la législation britannique proposée promet d'être moins onéreuse. 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.



Barracuda

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.

Extension des règles applicables aux grandes organisations chargées des infrastructures critiques aux petites entreprises et à celles qui sont considérées comme essentielles.

Les règles sont étendues aux entreprises de plus de 50 employés dans certains secteurs.

Les secteurs de l'énergie, des transports, des banques, de la santé, de l'infrastructure numérique, des fournisseurs de cloud computing, de la gestion des déchets, des producteurs de denrées alimentaires, d'une grande partie de l'industrie manufacturière, des moteurs de recherche et des organismes de recherche sont tous concernés.

Événement :

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

Les États membres doivent transposer la directive en droit national d'ici octobre 2024.

Notification obligatoire des incidents.

Comment ?

La cybersécurité relève clairement de la responsabilité de la haute direction, ce que fait la directive NIS2 en la rendant personnellement responsable 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 qui sont considérées comme essentielles.

Obligation de donner une alerte rapide en cas d'incident dans les 24 heures et de fournir une notification dans les 72 heures et un rapport détaillé dans un 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.

La conformité à la directive et la protection de l'entreprise impliquent d'identifier les besoins en termes de protection des appareils, des actifs et des 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. Vous devez notamment prouver 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 qui s'imposaient.

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 reconnaîtra les certifications européennes de produits et de solutions en matière de cybersécurité afin d'alléger la charge de travail des entreprises dans ce domaine. Si votre organisation respecte déjà 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.

Les sanctions prévues par la directive NIS2 sont lourdes, avec des amendes pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel total.

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

Gestion des risques liés à la cybersécurité : établissez des processus de gestion des risques pour gérer les risques informatiques et minimiser les menaces pesant sur les services critiques. Les États membres de l'UE et l'Agence de l'Union européenne pour la cybersécurité (ENISA) mèneront des évaluations coordonnées des risques de sécurité des chaînes d'approvisionnement critiques. Ces évaluations tiendront compte des facteurs de risque techniques et, le cas échéant, non techniques.

Responsabilité de l'entreprise : instaurez des mécanismes de notification interne afin de tenir la direction informée des risques et de la situation en matière de sécurité et de promouvoir ainsi la responsabilité. Mettez en place des structures permettant à la direction de l'entreprise de contrôler et d'approuver les mesures de cybersécurité et de faire face à tout risque informatique.

Obligations en matière de rapports : développez des capacités de rapports externes afin de répondre aux exigences stipulées par la NIS2 en termes de rapports d'incidents et d'éviter de lourdes pénalités. Établissez des procédures pour signaler rapidement les incidents de sécurité ayant un impact significatif sur la fourniture de services ou sur les destinataires. Les autorités compétentes peuvent alors évaluer l'impact de l'incident et guider les opérateurs ou les fournisseurs en question.

Continuité des activités : élaborez des plans qui doivent prendre en compte la gestion des sauvegardes, la reprise après sinistre et la gestion de crise afin d'assurer la continuité des activités en cas d'incidents informatiques.

Lignes directrices : procédez à des évaluations complètes des risques et mettez en œuvre des politiques rigoureuses en matière de sécurité des systèmes d'information. Cela garantira une approche proactive de l'identification et de l'atténuation de toute menace potentielle.

Gestion des incidents : établissez des processus de réponse aux incidents, effectuez des simulations et formez votre personnel pour qu'il soit prêt.

Chaîne d'approvisionnement : mettez en œuvre des mesures de sécurité pour vos chaînes d'approvisionnement et tissez une relation étroite entre l'organisation et ses fournisseurs directs en adaptant les mesures de sécurité à des vulnérabilités spécifiques. Effectuez fréquemment des évaluations générales de la sécurité de l'ensemble des fournisseurs afin de garantir un niveau élevé de sécurité tout au long de la chaîne d'approvisionnement.

Approvisionnement : renforcez la sécurité lors de l'approvisionnement, du développement et de l'exploitation des systèmes en mettant en œuvre un processus de gestion des vulnérabilités et en encourageant le traitement et le signalement de toute vulnérabilité qui se présente.

Contrôle quantitatif : instaurez des processus d'évaluation de l'efficacité des mesures de sécurité. Cela permettra d'assurer le suivi et l'amélioration continus des processus opérationnels dans le domaine de la cybersécurité.

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

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

Contrôle d'accès : mettez en œuvre des procédures de sécurité pour les employés ayant accès à des données confidentielles, y compris des politiques d'accès aux données.

Gestion des actifs : dressez un bilan de tous les actifs et biens de l'entreprise concernés et veillez à ce qu'ils soient correctement utilisés et traités à tout moment.

Authentification : adoptez l'authentification multifacteur (MFA) et l'évaluation continue de la confiance zéro, et appliquez le chiffrement de la voix, de la vidéo et du texte et, le cas échéant, des communications d'urgence internes afin de renforcer les mesures de sécurité.

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, reconnue par la nouvelle directive.

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, du réseau et des e-mails. Nous pouvons même vous fournir une solution XDR gérée pour superviser le tout.

Barracuda

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda. Nous pensons que chaque entreprise doit se doter de solutions cloud-first, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients. Plus de ~~220 000~~ 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business. Pour en savoir plus, rendez-vous sur fr.barracuda.com.

 Copyright 2024 Barracuda, Inc. • fr.barracuda.com
Barracuda et le logo Barracuda sont des marques déposées de Barracuda, Inc., États-Unis. Tous les autres noms appartiennent à leurs propriétaires respectifs.