RSA

Préparation à la directive NIS2 : Protéger les infrastructures critiques contre les cybermenaces

Ange Olivier AMBEMOU
Systems Engineer, RSA

OWN YOUR IDENTITY.

Table des matières

NIS1 versus NIS2 2
Quelles organisations doivent se conformer à NIS2 ? 2
Coopération et conformité 3
Suivez les directives de sécurité des identités ISO et NIST pour atteindre la conformité NIS2 3
"Ne jamais gaspiller une bonne crise" 3
Les plateformes d'identité dépassent les exigences de NIS2 4

Préparation à la directive NIS2 : Protéger les infrastructures critiques contre les cybermenaces

NIS1 versus NIS2

La directive NIS originale de 2016 était principalement axée sur l'établissement de mesures de cybersécurité de base pour protéger certains services interconnectés clés de l'UE. L'accent était mis sur l'infrastructure jugée essentielle (comme l'énergie, l'eau, les transports, les soins de santé et la banque) et couverte par les protections de base énoncées par la directive.

La directive NIS2 élargit le champ d'application de la directive NIS originale en englobant des secteurs et des entités supplémentaires. Elle couvre les opérateurs de services essentiels (OSE) dans des secteurs tels que l'énergie, les transports, la banque et les infrastructures des marchés financiers, les soins de santé, l'approvisionnement en eau et l'infrastructure numérique (comme les places de marché en ligne, l'informatique cloud et les moteurs de recherche), ainsi que les organisations qui soutiennent les OSE.

Les organisations incluses dans NIS2 doivent se conformer à ses directives d'ici le 17 octobre 2024. Il est dans l'intérêt des organisations de respecter ce délai : outre la fourniture de recommandations efficaces en matière de cybersécurité, NIS2 prévoit également des amendes pouvant atteindre 2 % du chiffre d'affaires mondial pour les organisations qui ne se conforment pas dans certaines situations.

Mais alors que NIS2 est clair sur qui doit suivre les directives et quelles sont les sanctions en cas de non-conformité, une chose qu'il ne définit pas est la manière dont les organisations doivent se préparer. Par conséquent, nous allons examiner les lignes directrices de NIS2 et les meilleures pratiques que les organisations devraient adopter pour respecter la conformité et se protéger contre les menaces émergentes.

Quelles organisations doivent se conformer à NIS2 ?

Pour mieux définir les organisations qui doivent être incluses, deux critères de base ont été établis : le secteur et la taille. Pour aborder le secteur, les annexes 1 et 2 de NIS2 identifient les secteurs "Hautement Critiques" (alias entités essentielles) et "Critiques" (alias entités importantes). Il existe onze secteurs Hautement Critiques, principalement ceux liés aux opérations quotidiennes de l'économie d'un pays, tels que l'énergie, les transports, la banque, les services d'eau, les soins de santé, l'infrastructure numérique, le gouvernement et l'espace. Les secteurs Critiques sont associés à des services clés qui soutiennent l'économie d'un pays, tels que la fabrication et la distribution de denrées alimentaires, de produits chimiques et de biens, la gestion des déchets, les fournisseurs numériques tels que les fournisseurs de services Internet (FAI) et la recherche.

Pour aborder la taille, NIS2 catégorise les organisations comme étant soit Grandes, soit de taille Moyenne. Les grandes organisations sont celles comptant plus de 250 employés et un chiffre d'affaires d'au moins 50 millions d'euros. Les organisations de taille moyenne sont celles comptant moins de 250 employés et un chiffre d'affaires annuel ne dépassant pas 50 millions d'euros.

Coopération et conformité

Pour aborder la coopération, NIS2 établit également une structure pour signaler les incidents. Cela inclut la formation de composants tels que l'autorité compétente, le point de contact unique et l'équipe de réponse aux incidents de sécurité informatique (CSIRT). L'article 23 énonce ce qui doit être signalé et les délais.

L'application est définie par l'adhésion des organisations à la mise en œuvre des Mesures de Gestion des Risques en Cybersécurité recommandées et des exigences de déclaration. Les amendes pour non-conformité pour ces entreprises peuvent aller jusqu'à 10 millions d'euros (ou jusqu'à 2 % du chiffre d'affaires mondial) pour les entités Hautement Critiques ou 7 millions d'euros pour les entités Critiques.

Suivez les directives de sécurité des identités ISO et NIST pour atteindre la conformité NIS2

D'ici le 17 octobre 2024, les États membres doivent adopter et publier les mesures nécessaires pour se conformer à la directive NIS2. Mais que cela signifie-t-il exactement pour les entreprises concernées ?

NIS2 énumère les mesures clés que les secteurs et les organisations d'infrastructures numériques dans toute l'UE doivent mettre en œuvre, notamment l'utilisation de l'authentification multi-facteurs (MFA), des politiques de contrôle d'accès et de gestion d'actifs, une hygiène de base en matière de cybersécurité et une formation, entre autres mesures.

NIS2 ne définit pas comment atteindre ces mesures. Au lieu de cela, il renvoie à d'autres normes telles que l'ISO, CIS, NIST ou IEC, ainsi qu'aux principes du "zéro trust", comme des lignes directrices que les organisations devraient suivre pour atteindre la conformité.

Ces normes accordent la priorité à la sécurité des identités. Par exemple, la norme ISO27002 sur la sécurité de l'information, la cybersécurité et la protection de la vie privée fournit des conseils utiles sur l'avancement du contrôle d'accès, de la gestion des identités, de l'authentification sécurisée et d'autres capacités qui s'alignent avec NIS2. NIS2 recommande également les sept principes du "zéro trust" de NIST, qui mettent également l'accent sur les contrôles de sécurité des identités.

En suivant ces deux approches, les organisations concernées disposeront d'une méthodologie approfondie pour atteindre la conformité NIS2 et se protéger contre les cyberattaques les plus fréquentes et les plus dommageables.

"Ne jamais gaspiller une bonne crise"

Il existe un vieux dicton selon lequel les organisations ne devraient jamais gaspiller une bonne crise, et c'est le cas avec NIS2, qui oblige les organisations à évaluer tous les aspects de leurs protocoles de sécurité et à se concentrer sur les principes du "zéro trust" et les normes pertinentes qui s'appliquent à leur entreprise. En le faisant, les organisations ne devraient pas aborder NIS2 comme un exercice de coche : s'ils prennent le temps d'évaluer leur posture en matière de cybersécurité, alors ils devraient investir dans les capacités qui défendent contre les attaques les plus fréquentes et les plus graves.

Dans la plupart des cas, il s'agit de l'identité. Le rapport d'enquête sur les violations de données de Verizon de 2023 a révélé que les "trois principales façons dont les attaquants accèdent à une organisation sont les identifiants volés, le phishing et l'exploitation des vulnérabilités." De plus, l'utilisation d'identifiants volés "est devenue le point d'entrée le plus populaire pour les violations" au cours de l'année dernière ; le rapport a constaté que 49% de toutes les violations de données impliquaient des identifiants.

Ce n'est pas seulement que l'identité soit le domaine compromis dans la plupart des attaques - c'est aussi que les attaques liées à l'identité tendent à coûter le plus cher aux organisations. Le rapport sur le coût d'une

violation de données d'IBM de 2023 a révélé que le vecteur d'attaque initial le plus fréquent était le phishing ; c'était aussi l'un des plus coûteux, coûtant en moyenne 4,76 millions de dollars aux organisations.

Les plateformes d'identité dépassent les exigences de NIS2

Bien que tous les domaines de sécurité soient importants, l'identité, en particulier dans l'environnement de travail hybride, joue un rôle clé dans la sécurisation de votre organisation. Les organisations devraient désigner un partenaire de sécurité axé sur l'identité pour mener une évaluation de NIS2 et recommander le meilleur mélange d'intelligence d'identité automatisée, d'authentification, de gestion des accès, de gouvernance et de solutions de cycle de vie pour vous permettre de protéger toutes les ressources, identités et environnements définis par la directive NIS2.

Les organisations constateront qu'une plateforme d'identité unifiée sera le moyen le plus simple de garantir une revue complète de bout en bout et un ensemble de solutions qui peuvent être établies pour dépasser toutes les exigences de NIS2 et évoluer pour répondre aux besoins futurs alors que les exigences commerciales et de sécurité évoluent.

Pour en savoir plus, contactez RSA pour commencer votre évaluation de sécurité de l'identité NIS2.