Checklist de mise en conformité à la directive NIS2 :

7 étapes pour vous préparer

La directive NIS2 de l'Union européenne introduit de nouvelles obligations pour les entreprises, qui doivent renforcer leur cybersécurité, procéder à des audits réguliers et signaler rapidement les incidents. La conformité est obligatoire pour les organisations proposant des services essentiels, mais elle est aussi cruciale pour celles espérant devenir leurs fournisseurs. Préparez la conformité de votre entreprise à la directive NIS2 grâce à des mesures clés.

1 Identifiez vos risques de cybersécurité

Des vulnérabilités peuvent être dissimulées dans votre réseau, vos systèmes et vos actifs, vous exposant à des risques. Par exemple, les mots de passe non gérés, ou les comptes mal configurés ou inactifs, sont susceptibles d'entraîner des vols d'identifiants. Réalisez une évaluation complète de la sécurité pour identifier les problèmes, évaluer leur impact et commencer à prendre des mesures pour les corriger.

Mesure clé

Réalisez une évaluation des risques à l'échelle de l'entreprise et élaborez un plan de réduction des vulnérabilités.

2 Renforcez le contrôle des accès

Il est essentiel de bloquer les accès non autorisés aux systèmes et aux comptes utilisateurs pour prévenir les compromissions de données. Appliquez des mesures robustes de contrôle des accès grâce à une plateforme d'identité performante qui centralise la gestion des utilisateurs et vous permet de définir des politiques d'autorisation granulaires, afin que seules les personnes autorisées puissent accéder à des ressources spécifiques ou réaliser certaines actions.

Mesure clé

Implémentez une gouvernance des identités robuste pour appliquer un contrôle plus strict des accès.

3 Protégez les accès à privilèges

Les cybercriminels peuvent exploiter des comptes à privilèges pour orchestrer des attaques, paralyser des infrastructures critiques et perturber des services essentiels. Protégez les accès à privilèges en limitant l'accès aux comptes administrateur et en imposant la modification régulière des mots de passe administrateur.

Mesure clé

Protégez les comptes à privilèges grâce à de bonnes pratiques telles que l'accès sur le principe du moindre privilège.

4 Implémentez un MFA résistant au phishing

Face à l'essor des attaques de social engineering, la directive NIS2 exige des organisations qu'elles implémentent une authentification multifacteur (MFA) résistante au phishing. Cette dernière offre une couche de sécurité supplémentaire lors de l'authentification des collaborateurs, des clients et des prestataires, sans ajouter de points de friction à leur expérience numérique.

Mesure clé

Déployez un MFA résistant au phishing pour renforcer l'authentification sans créer de points de friction.

5 Renforcez vos défenses contre les ransomwares

Coûteuses et paralysantes, les attaques de ransomware sont l'un des principaux moteurs de la directive NIS2. Adoptez des solutions de sécurité pour vous défendre de façon proactive contre ces attaques, comme une solution de gestion des endpoints à privilèges pour appliquer le principe du moindre privilège, contrôler les applications et renforcer les antivirus de nouvelle génération et les solutions EDR.

Mesure clé

Adoptez des solutions de sécurité pour vous défendre de façon proactive contre les ransomwares, comme une solution de gestion des endpoints à privilèges.

6 Inspectez votre chaîne logistique logicielle

Les logiciels d'éditeurs tiers que vous utilisez peuvent être infectés par du code malveillant. Posez un regard neuf sur votre chaîne logistique logicielle et envisagez d'implémenter une solution de gestion des secrets pour stocker en toute sécurité des données sensibles, comme des mots de passe, des clés et des jetons.

Mesure clé

Envisagez d'implémenter une solution de gestion des secrets afin de réduire le risque d'attaques de la chaîne logistique.

7 Adoptez une stratégie Zero Trust

Les architectures de sécurité traditionnelles basées sur le périmètre ne sont pas adaptées aux services cloud et aux effectifs hybrides. Envisagez d'adopter une approche Zero Trust multicouche, reposant sur une gestion des identités robuste, qui applique l'accès sur le principe du moindre privilège, l'authentification continue et l'analyse des menaces.

Mesure clé

Adoptez une stratégie Zero Trust axée sur l'identité qui accorde aux bonnes personnes l'accès aux ressources pertinentes au bon moment.

En savoir plus sur l'identité et la directive NIS2

L'identité est le fondement de l'accès aux informations critiques. Par le biais d'une gestion sécurisée des identités, les entreprises peuvent contrôler les accès, renforcer l'authentification et établir la responsabilité avec une piste d'audit facilement accessible.

Pour en savoir plus sur la façon dont l'identité permet la conformité à la directive NIS2, lisez le livre blanc **L'importance de l'identité pour préparer la conformité à la directive NIS2**.

Télécharger

okta