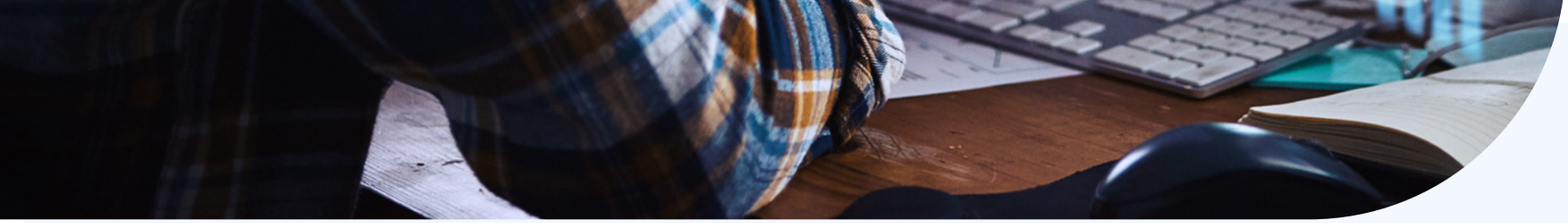
Votre système de contrôle d'accès physique est-il **conforme à la directive NIS2 ?**

Cette nouvelle réglementation européenne vise à harmoniser la sécurité physique et la cybersécurité pour une protection renforcée.

EBOOK



Enjeux et points clés de la directive NIS2

La cybersécurité affecte aussi bien les entreprises que les individus et les gouvernements. Dans un environnement où les menaces évoluent constamment, il est essentiel de rester vigilant. Pour répondre à ces nouveaux défis, les gouvernements mettent en place de nouvelles régulations visant à mieux protéger les données sensibles et assurer la sécurité des utilisateurs.

C'est dans ce contexte que l'Union Européenne a adopté la **Directive sur la sécurité des réseaux et des systèmes d'information (NIS2)**, une mise à jour de la directive NIS de 2016, visant à sécuriser les infrastructures critiques. La directive est effective depuis le **17 octobre 2024**.

Depuis cette date, tous les États membres doivent avoir intégré les exigences de la directive NIS2 dans leurs législations nationales, et les entreprises sont tenues de s'y conformer sous peine de lourdes sanctions.

La directive NIS2 vise à renforcer la résilience face aux menaces physiques et numériques, tout en garantissant une récupération rapide des systèmes et infrastructures IT (technologies de l'information) et OT (technologies opérationnelles).

NIS2: des exigences adaptées à chaque pays

La directive NIS2 définit un niveau d'exigences **minimum**, que chaque état adaptera. Par exemple, les infrastructures critiques devront signaler tout incident majeur à l'autorité nationale compétente dans un délai de 24 heures, mais chaque pays désigne l'autorité à contacter. Cependant, beaucoup de ces détails sont encore en cours d'élaboration et peuvent évoluer.

Les nouveautés de la directive NIS2 :

des mesures de sécurité renforcées, des amendes plus sévères, des obligations de déclaration accrues et un focus sur la supply chain

La directive NIS2 a été conçue pour renforcer et moderniser le cadre juridique initialement établi dans la première. Elle vise à améliorer la résilience et la sécurité des infrastructures numériques critiques au sein de l'Union européenne, en répondant aux nouvelles menaces cybernétiques et en harmonisant les règles entre les États membres.

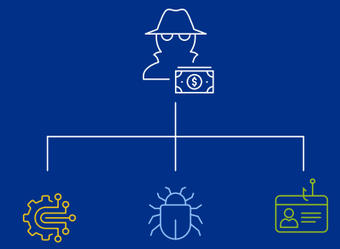
Voici quelques-unes des évolutions notables:

- **Davantage de secteurs concernés :** la directive NIS2 intègre désormais des secteurs essentiels comme l'énergie, les transports, la finance, la santé, les services publics, les infrastructures numériques ou encore l'administration publique. Même les organisations affichant un chiffre d'affaires annuel brut de 10 millions d'euros devront se conformer à ces nouvelles exigences. **Pour une liste complète des secteurs, sous-secteurs et catégories d'entités, consultez l'Annexe 1.**
- **Inclusion des fournisseurs :** la directive NIS2 distingue les « entités essentielles » (EE) et les « entités importantes » (EI). Ainsi, toute entreprise faisant partie de la chaîne d'approvisionnement d'une EE ou d'une EI doit également respecter cette réglementation. Par conséquent, certains sites de fabrication de HID pourraient être classés comme EI. Pour découvrir les mesures mises en place afin que ces installations soient des références en matière de cybersécurité, rendez-vous à la page 6.
- **Contrôles renforcés :** la nouvelle directive impose des mesures de sécurité plus strictes, incluant la prévention des accès non autorisés et les cybermenaces. Les organisations devront mettre en place des contrôles fiables pour réduire les risques et protéger leurs systèmes et données.
- **Obligation de déclaration :** les incidents majeurs doivent être signalés dans les 24 heures suivant leur détection. Qu'est-ce qu'un « incident majeur » ? D'après la directive, il s'agit de tout événement pouvant entraîner des dommages, des perturbations ou des pertes graves, pour votre organisation ou pour des tiers.
- **Sanctions plus sévères :** les amendes pour non-conformité peuvent désormais atteindre jusqu'à 10 % du chiffre d'affaires annuel.

Évaluation des risques : une étape clé

La directive NIS2 vise à renforcer la résilience en matière de cybersécurité. La résilience ne se construit pas du jour au lendemain, c'est pourquoi la législation met l'accent sur des évaluations et des processus adaptés à chaque entreprise.

La première étape consiste à réaliser une évaluation des risques opérationnels afin d'identifier les menaces susceptibles de perturber les services essentiels proposés par l'entreprise. Cette évaluation doit être mise à jour régulièrement et accompagnée de mesures concrètes pour réduire les risques, sous peine de responsabilité personnelle.



L'augmentation des risques : mythe ou réalité ?

Une réalité.

En 2023, l'Agence européenne pour la cybersécurité (ENISA) a constaté une augmentation notable du nombre de cyberattaques. Les types de cyberattaques sont variés : Les attaques par déni de service distribué (DDoS) et les ransomwares figurent en tête de liste, suivies des attaques d'ingénierie sociale, des menaces liées aux données, de la manipulation d'informations, des cybermenaces dans la chaîne d'approvisionnement et des malwares.

La directive NIS2 aborde et intègre l'interdépendance entre la sécurité physique et la cybersécurité

La frontière entre le monde physique et le numérique s'estompe peu à peu. Le **Rapport 2024 sur l'état du contrôle d'accès physique**, publié par HID en collaboration avec IFSEC Insider, met en lumière plusieurs tendances importantes :

- Près de la moitié des répondants **(48 %)** affirment que le département informatique est pleinement impliqué dans la mise à niveau des systèmes de contrôle d'accès physique.
- **58 %** des équipes de sécurité collaborent avec le département informatique pour définir les meilleures pratiques en matière de sécurité, tandis que
- **55 %** des professionnels de la sécurité déclarent collaborer avec le département informatique

Gartner confirme cette tendance, en indiquant que 41 % des entreprises prévoient de combiner la cybersécurité et la sécurité physique d'ici 2025, soit une hausse de 10 % par rapport à 2020.

La sécurité d'une entreprise n'est jamais plus forte que son maillon le plus faible, qu'il soit physique ou numérique. L'interconnexion de ces systèmes offre de nombreux avantages, mais elle expose également à des vulnérabilités. Imaginez un système de contrôle d'accès compromis : il pourrait permettre à des individus malveillants de modifier les autorisations, désactiver des alarmes ou encore dérober des informations sensibles.

De nombreux systèmes de contrôle d'accès en place aujourd'hui sont obsolètes et représentent des risques considérables. Voici quelques statistiques révélées dans le rapport 2024 sur l'état du contrôle d'accès physique :

- **42 %** des entreprises utilisent un système de contrôle d'accès datant de moins de 3 ans
- **14 %** utilisent leur système de contrôle d'accès qui a plus de 6 ans
- **54 %** prévoient de mettre à jour leur logiciel de contrôle d'accès
- **53 %** souhaitent mettre à jour leurs lecteurs et identifiants
- **50 %** envisagent de remplacer leurs contrôleurs

L'intégration des technologies IT et OT est devenue indispensable pour obtenir une vue d'ensemble de vos opérations et réduire les menaces croissantes liées aux systèmes et dispositifs interconnectés.

Renforcer la cybersécurité de votre système de contrôle d’accès physique

Pour garantir la sécurité de votre système de contrôle d'accès, il est essentiel de considérer l'intégrité de l’ensemble des composants. Une évaluation des risques NIS2 doit inclure une analyse des flux d'informations, en s’assurant que les données sensibles sur les identités et les droits d’accès sont correctement gérées et protégées.

Nous recommandons d'adopter une approche progressive, en établissant d’abord une configuration initiale solide avant d'envisager des améliorations. Vous pouvez visionner notre webinaire à la demande, ou bien consulter ci-dessous les procédures pour chaque type de produit :

Identifiants

- **Fonction :** Stocker les données de contrôle d'accès de manière sécurisée
- **Configuration initiale :** Optez pour des cartes intelligentes ou virtuelles avec des données protégées par un chiffrement robuste (AES 128).
- **Optimisation de la sécurité :** Renforcez la sécurité avec des politiques de gestion des identifiants des solutions certifiées.

Lecteurs

- **Fonction :** Traiter et transmettre les identifiants à un contrôleur
- **Configuration initiale :** Mettez en place des lecteurs sécurisés capables de traiter les cartes chiffrées et de stocker des clés de chiffrement.
- **Optimisation de la sécurité :** Sécurisez la communication entre le lecteur et le contrôleur en vous basant sur la norme IEC 60839-11-5:2020 OSDP v2. Gérez les mises à jour via des applications de maintenance autorisées.

Contrôleurs

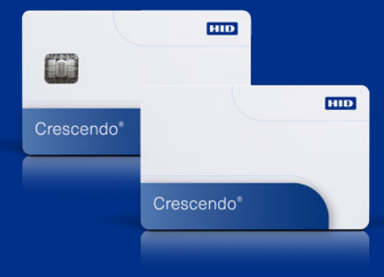
- **Fonction :** Communiquer avec les lecteurs et les cartes afin de vérifier les autorisations des utilisateurs pour l'accès à des zones spécifiques
- **Configuration initiale :** Installez les contrôleurs dans des environnements sécurisés, sur un VLAN dédié, et désactivez toutes les interfaces non essentielles. N’oubliez pas de tenir à jour le firmware et les correctifs.
- **Optimisation de la sécurité :** Permettez uniquement aux adresses IP approuvées de se connecter au contrôleur et veillez à utiliser le chiffrement pour protéger les données.

Clients et serveurs de contrôle d’accès

- **Fonction :** Servir de base de données principale et de console de gestion du système, enregistrer les activités et permettre aux organisations d'ajuster les paramètres
- **Configuration initiale :** Assurez-vous que les serveurs et les clients soient hébergés sur un VLAN dédié et sécurisé, en mettant à jour régulièrement les correctifs. Choisissez une solution qui offre un reporting transparent des Vulnérabilités et Expositions Communes (CVE) et qui respecte les normes du Cycle de Vie de Développement de Logiciel (SDLC), telles que l'ISA/IEC 62443-4-1.
- **Optimisation de la sécurité :** Protégez les données stockées et en transit avec des certificats TLS personnalisés.

HID votre partenaire pour accompagner votre transformation digitale

Bien que cet eBook se concentre principalement sur la conformité aux exigences d’accès physique de la directive NIS2, il est essentiel de rappeler qu'HID est un leader mondial dans la gestion des identités et l'authentification, notamment avec des solutions d'authentification multifactorielle (MFA), fortement recommandées dans le cadre de la directive NIS2.



Faites confiance à notre expertise

HID est un partenaire de choix pour les « entités essentielles » et « importantes », avec plusieurs sites de production classés comme critiques selon la directive NIS2. Pour garantir l'excellence en matière de cybersécurité, nous avons mis en place plusieurs mesures :

- **Certifications au-delà des exigences NIS2 :** Nos usines et nos processus de développement dépassent largement les standards de la directive. Avec des certifications comme SOC2 Type 2, ISO 27001, ISO 27018, CSA Star Level 2 et SEAL-5 TÜV, nous allons au-delà des exigences minimales et offrons une sécurité optimale.
- **Amélioration continue :** Nous restons à l'affût des nouvelles réglementations pour adapter nos pratiques et offrir à nos clients des solutions à la pointe de la cybersécurité.
- **Protection inter-opérable complète :** Notre approche englobe tous les aspects de la sécurité, de la gestion des accès physiques à celle des identités numériques, en intégrant des certificats numériques et des solutions biométriques.
- **Une expertise reconnue dans le monde entier :** Depuis plus de 30 ans, HID est le partenaire de confiance des secteurs hautement sécurisés comme les gouvernements, les banques et les établissements de santé.

Votre sécurité, notre priorité

Chaque jour, des millions d'utilisateurs dans plus de 100 pays font confiance à HID pour sécuriser leurs environnements physiques et numériques. Nos solutions sont conçues pour vous aider à respecter la directive NIS2.

Chez HID, nous nous engageons à protéger votre entreprise, vos données et vos équipes.

Certifications

AICPA SOC

ISO 27001 CERTIFIED by schellman

ISO 27018 CERTIFIED by schellman

CSA cloud security alliance®

TÜVIT 2020 Trusted Product

© TÜVIT – TÜV NORD GROUP – www.tuvit.de

HID

hidglobal.com

Amérique du Nord : +1 512 776 9000
Numéro gratuit : 1 800 237 7769
Europe, Moyen-Orient, Afrique : +353 91 506 900
Asie-Pacifique : +852 3160 9800
Amérique latine : +52 55 9171-1108

Pour obtenir d'autres numéros de téléphone internationaux, cliquez ici

2024-10-03-pacs-nis2-eb-fr
PLT-08079

Groupe ASSA ABLOY