EVVA
access to security

Whitepaper

La première ligne de défense
Contrôle d'accès aux infrastructures critiques

La première ligne de défense Contrôle d’accès aux infrastructures critiques

Comment les systèmes modernes de contrôle d’accès contribuent au respect des normes NIS2 et CER – et renforcent durablement la sécurité physique.

Le contrôle d’accès, élément clé de la conformité aux normes NIS2 et CER

Le monde et nous aussi avons changé – surtout ces dernières années. Des changements géopolitiques comme les guerres, l’instabilité politique, les modifications climatiques et les nouvelles technologies influencent notre quotidien et demandent plus de résilience de la part des infrastructures vitales, surtout une augmentation de la protection physique.

Avec la directive européenne NIS2 (2022/2555) et la directive complémentaire CER (2022/2557), l’Union européenne renforce considérablement les exigences de sécurité imposées aux exploitants d’infrastructures critiques et importantes. Ces deux réglementations ont pour objectif de renforcer de manière globale la résilience face aux menaces numériques et physiques, ce qui place également le contrôle d’accès au cœur des architectures de sécurité modernes. Dans ce livre blanc, nous souhaitons nous intéresser principalement au thème des « mesures de protection physique des infrastructures critiques ».

Cadre réglementaire : NIS2 et CER

Les définitions

NIS2 et CER sont des directives européennes qui doivent être transposées dans la législation nationale ; vous trouverez un aperçu clair des désignations légales correspondantes sur les marchés européens à la page 15 du livre blanc.

NIS2

Cybersécurité pour les secteurs critiques et essentiels

- EU-Directive européenne (2022/2555)
- **Objectif :** renforcer le niveau de cybersécurité grâce à des normes minimales à l'échelle de l'UE. Oblige les entreprises et les organisations à améliorer systématiquement leur sécurité informatique et leur cybersécurité, et à signaler les incidents.
- **S'applique aux :**
  - aux entités «essentielles» : cela inclut les entreprises à haut niveau de criticité dont la défaillance aurait des répercussions considérables sur la société, l'économie ou la sécurité publique, notamment les secteurs de l'énergie, des transports, des banques, de la santé, de l'eau, des télécommunications et des technologies de l'information
  - **aux secteurs «importants» :** cela inclut les entreprises ayant d'autres répercussions critiques, telles que la poste, la gestion des déchets, l'industrie chimique, l'agroalimentaire et la fabrication de biens (à partir de 50 salariés et 10 millions d'euros de chiffre d'affaires)
- **Les exigences imposées aux entreprises relevant de la directive NIS-2 comprennent notamment :**
  - la gestion de la cybersécurité (analyses des risques, stratégies de sécurité, réponse aux incidents, continuité des activités)
  - l'obligation de signaler les incidents de sécurité
  - la responsabilité de la direction
  - une surveillance stricte et des sanctions

CER

Résilience physique des infrastructures critiques

- Directive de l'UE (2022/2557)
- **Objectif :** renforcer la résilience physique face aux menaces et dangers non numériques (approche « tous les risques »)
- **S'applique aux :** opérateurs d'infrastructures critiques tels que :
  - Énergie
  - Transports
  - Banques
  - Santé
  - Eau
  - Télécommunications/informatique
  - Agroalimentaire
  - Industrie chimique
- Exigences :
  - Analyses des risques
  - Plans d'urgence et de reprise d'activité
  - Mesures de sécurité
  - Gestion de la chaîne d'approvisionnement et des dépendances
  - Obligation de signalement des incidents graves
  - Garantie de la continuité des services essentiels

En bref

En résumé, cela signifie que les entités concernées par la directive NIS2 et le règlement CER doivent, après avoir procédé à une analyse systématique des menaces et des risques, ainsi qu'à une évaluation, mettre en œuvre des mesures visant à assurer une protection physique efficace. Cela comprend notamment le contrôle d'accès, la surveillance et les procédures de détection des incidents.Le CER précise encore ces dispositions : les exploitants d'installations critiques doivent réaliser des analyses de risques tous les quatre ans, mettre en œuvre des mesures de protection physique appropriées et empêcher efficacement tout accès non autorisé.

La cybersécurité passe aussi par une protection physique

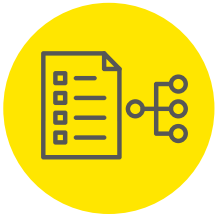
Caractéristiques de sécurité pertinentes pour une utilisation dans les environnements NIS2 et CER

Sécurité physique des accès

- Contrôle d'accès strict aux zones critiques
- Supports d'accès infalsifiables
- Technologies de pointe

Sécurité informatique et cryptage

- Communication sécurisée grâce aux normes de cryptage actuelles (TLS, AES, ECDSA)
- Pas de mots de passe non sécurisés



Journalisation et audits

- Documentation complète de tous les accès et de toutes les actions effectuées sur le système
- Journaux conformes aux exigences d'audit, avec fonction d'exportation sous forme de document d'audit

Réponse aux incidents et protection des accès

- Blocage rapide des accès compromis
- Plans d'urgence en cas de panne ou d'attaque (fonctionnement hors ligne des portes)

Continuité des activités et sauvegarde des données

- Stratégie automatisée de sauvegarde des donnéesStratégie de reprise après sinistre, redondance

Gestion des vulnérabilités et mises à jour

- Suivi continu des failles de sécurité logicielles (CVE) par les éditeurs
- Mises à jour rapides, signées et vérifiées

Protection des données et sécurité des données

- Confidentialité dès la conception, conformité au RGPD
- Fonctions de suppression des données à caractère personnel
- Journalisation configurable
- Principe du double contrôle pour la consultation des journaux

Les produits EVVA et leur conformité aux exigences réglementaires

Xesar

Système d'accès répondant aux exigences de sécurité les plus strictes

Sécurité physique et informatique

- Droits d'accès basés sur les rôles par personne/groupe
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), clés AES spécifiques à chaque installation
- Communication « challenge-response » chiffrée (pas de protocoles en clair)
- TLS ≥ 1.2 pour la communication système
- Chiffrement interne AES 256 bits
- Mots de passe hachés (Bcrypt)

Journaux d'accès et journaux système

- Journaux d'événements et de système complets et inviolables
- Exportations conformes aux exigences d'audit
- Preuves d'audit et d'incidents disponibles à tout moment

Réponse aux incidents et résilience

- Blocages en temps réel (en ligne), listes de blocage pour les composants hors ligne
- Mécanismes d'alerte en cas d'état de blocage incertain
- Fonctionnement autonome hors ligne en cas de panne informatique ou réseau

Mises à jour et gestion des vulnérabilités

- Surveillance continue des vulnérabilités CVE
- Mises à jour signées cryptographiquement (RSA/SHA256, AES256CCM)
- Mises à jour vérifiées du micrologiciel et des logiciels

Continuité des activités

- Sauvegardes chiffrées
- Restauration d'urgence via la fiche de sécurité du système
- Possibilité d'utilisation multi-postes et de fonctionnement du serveur 24 h/24, 7 j/7

Protection des données

- Confidentialité dès la conception
- Aucune donnée à caractère personnel dans l'application
- Suppression automatique des données à caractère personnel configurable

AirKey

Solution d'accès mobile répondant aux normes les plus strictes

Sécurité physique et informatique

- Supports d'accès basés sur smartphone et RFID (JCOP SmartMX3, EAL6+)
- Authentification ECDSA256 + clés de session AES
- Gestion en ligne sécurisée par TLS

Journaux d'accès et journaux système

- Journalisation conforme aux exigences d'audit
- Exportations conformes aux exigences d'audit
- Mise à jour automatique des listes noires et des journaux
- Configuration flexible et conforme à la réglementation en matière de protection des données

Réponse aux incidents et résilience

- Verrouillages en temps réel via Internet
- Fonctionnement hors ligne de la porte même en cas de panne du serveur
- Avertissements en cas de situations critiques pour la sécurité

Mises à jour et fonctionnement

- Gestion centralisée et signée des mises à jour
- Centres de données certifiés ISO 27001 en Autriche
- Serveurs EVVA redondants, clés sécurisées par HSM

Protection des données

- Stratégies de suppression conformes au RGPD
- Privacy by Design
- Principe du double contrôle pour la consultation des journaux activable

NORMES ET STATUT DE CERTIFICATION

A passé avec
succès le contrôle
technique (TÜV)

EN 18031-1

EXIGENCES RED* RESPECTÉES

*RED: Directive relative aux équipements radioélectriques

Exemple pratique n° 1 :

Contrôle d'accès dans un hôpital

NIS2/CER-pertinent

Contexte

Un hôpital fait partie des « infrastructures essentielles » au sens de la directive NIS2 et est soumis à des exigences strictes en matière de sécurité informatique et physique. Les zones particulièrement sensibles, telles que les salles de serveurs, les entrepôts de médicaments ou les unités de soins intensifs, doivent être protégées contre tout accès non autorisé.

Solution avec Xesar

- Droits d'accès basés sur les rôles pour différents groupes de collaborateurs (par exemple : informatique, soins, administration)
- Supports d'accès dotés de technologies individuelles hautement sécurisées (MIFARE DESFire EV3)
- Enregistrement complet de tous les accès, journaux conformes aux exigences d'audit
- Blocage rapide des supports perdus via des listes de blocage en temps réel
- Fonctionnement hors ligne des portes en cas de panne du serveur (continuité d'activité)
- Mises à jour logicielles régulières et signées, et gestion des vulnérabilités

Valeur ajoutée

L'hôpital met en œuvre des mesures fondées sur les risques, est en mesure de documenter de manière exhaustive les incidents et renforce ainsi la résilience physique de cet établissement.

Exemple pratique n° 2 :

Site de production en tant que sous-traitant pour les infrastructures critiques

Chaîne d'approvisionnement / Pertinent pour le CER

Contexte

Une entreprise de taille moyenne spécialisée dans la construction mécanique fournit des fournisseurs d'énergie et relève donc indirectement de la directive CER. L'entreprise doit démontrer que ses systèmes d'accès et son infrastructure informatique sont résilients et sécurisés.

Solution avec AirKey

- Les droits d'accès sont gérés de manière centralisée, y compris pour les prestataires externes (par exemple, le personnel de maintenance)
- Application sécurisée basée sur le cloud
- Supports d'accès (smartphones, RFID) dotés d'un cryptage très élevé (ECDSA-256, AES-128)
- Enregistrement de tous les accès, exportation à des fins d'audit
- Fonctions de suppression conformes au RGPD et « Privacy by Design »
- Mises à jour et gestion des vulnérabilités centralisées par EVVA

Valeur ajoutée

L'entreprise peut démontrer à ses clients qu'elle a mis en œuvre les mesures appropriées pour garantir la sécurité de la chaîne d'approvisionnement en matière d'accès et qu'elle est parfaitement préparée pour les audits et les certifications.

Exemple pratique n° 3 :

Gestion des situations d'urgence et résilience au sein d'une administration municipale

CER-pertinent

Contexte

Une administration municipale gère des infrastructures critiques (par exemple, l'approvisionnement en eau et les stations d'épuration) et doit veiller à ce que, en cas d'urgence (par exemple, une cyberattaque ou une coupure de courant), l'accès aux zones importantes reste possible.

Solution avec Xesar

- Fonctionnement hors ligne assuré en cas de coupure de courant ou de cyberattaque
- Blocage rapide des supports d'accès compromis, alertes en cas de tâches de sécurité en suspens
- Fonctions de sauvegarde et de restauration des données de configuration

Valeur ajoutée

Même en cas de crise, l'administration municipale reste opérationnelle : les habitants et les entreprises implantées sur le territoire ne sont pas affectés par les pannes et les perturbations.

Exemple pratique n° 4 :

Protection des données et journalisation dans un institut de recherche

NIS2/CER-pertinent

Contexte

Un institut de recherche traite des données à caractère personnel sensibles et doit se conformer au RGPD ainsi qu'aux exigences de la directive NIS2.

Solution avec AirKey

- Privacy by Design : aucune conservation de données à caractère personnel dans le backend
- Journalisation configurable, fonctions de suppression des données à caractère personnel
- Mise en œuvre conforme au RGPD

Valeur ajoutée

L'institut est en mesure de prouver à tout moment le respect de la protection des données et de la transparence vis-à-vis des autorités de contrôle et de ses partenaires.

Bilan de sécurité pour les exploitants d'infrastructures critiques

1. Cadre organisationnel de sécurité

- Disposons-nous d'un dispositif de sécurité contraignant pour garantir la sécurité physique ?
- Existe-t-il des structures clairement définies en matière de rôles, de droits et de responsabilités pour la sécurité, l'informatique, les installations et les domaines relevant de la réglementation KRITIS ?
- Les directives et processus de sécurité sont-ils régulièrement revus et mis à jour ?
- Le respect de l'obligation de signalement des incidents de sécurité est-il garanti par des procédures ?

2. Analyse des risques et conformité

- Avons-nous réalisé, au cours des quatre dernières années, une analyse des risques conformément à la loi-cadre KRITIS/CER ?
- Avons-nous identifié toutes les vulnérabilités physiques et numériques tout au long de la chaîne de processus ?
- Nos solutions d'accès sont-elles conformes à la directive NIS2, notamment en matière de protocoles sécurisés et de protection contre la manipulation ?
- Utilisons-nous exclusivement des systèmes à la pointe de la technologie (pas de protocoles non chiffrés tels que Wiegand, par exemple) ?

3. Droits d'accès et identités

- Les autorisations d'accès sont-elles toutes attribuées en fonction des rôles et de manière traçable ?
- Les droits d'accès font-ils l'objet d'une recertification régulière ou sont-ils automatiquement retirés lorsqu'ils ne sont plus nécessaires ?
- Disposons-nous de processus clairs pour l'intégration, le changement de rôle et le départ des collaborateurs et des prestataires ?

4. Sécurité technique du contrôle d'accès

- Tous les lecteurs d'accès, cartes et supports d'identification sont-ils cryptés ?
- Toutes les portes, salles de serveurs et postes de contrôle critiques pour la sécurité sont-ils protégés par des systèmes d'accès électroniques ?
- Les données sensibles en matière de sécurité (par exemple, les journaux) sont-elles stockées de manière à pouvoir faire l'objet d'un audit et protégées contre toute manipulation ?

5. Surveillance, journalisation et transparence

- Tous les accès et toutes les tentatives d'accès sont-ils automatiquement consignés ?
- Nos journaux d'accès sont-ils conformes aux exigences d'audit, protégés contre toute altération et conservés pendant une durée suffisante ?
- Utilisons-nous des outils de surveillance qui relient les événements de sécurité physiques et numériques ?

6. Protection des zones critiques

- Les zones telles que les salles de serveurs, les centres de contrôle, les installations énergétiques et d'approvisionnement ou les armoires électriques bénéficient-elles d'une protection particulière ?
- Existe-t-il des zones d'accès à plusieurs niveaux avec un niveau de sécurité croissant ?
- Les locaux sensibles sont-ils sécurisés en plus par une vidéosurveillance, une surveillance de l'état des portes ou un système d'alarme ?
- Disposons-nous d'un plan d'accès d'urgence (par exemple en cas de coupure de courant ou de panne du système) ?

7. Fournisseurs et prestataires de services

- Les entreprises et prestataires externes disposent-ils uniquement de droits d'accès limités dans le temps et clairement définis ?
- Les accès destinés au personnel temporaire font-ils l'objet de restrictions techniques et d'une surveillance stricte ?
- L'utilisation des accès externes fait-elle l'objet d'audits réguliers ?

8. Capacité de gestion des urgences et de reprise après sinistre

- Existe-t-il un plan de gestion des urgences et des crises qui inclut les aspects liés à la sécurité physique ?
- Des procédures ont-elles été définies pour :
  - le blocage immédiat de l'accès de certains utilisateurs ou groupes
  - la restauration rapide de l'infrastructure d'accès après une attaque
  - les scénarios d'évacuation ou d'intervention en cas d'incident
- Ces plans font-ils l'objet d'exercices réguliers ?

9. Formation et sensibilisation

- Tous les collaborateurs reçoivent-ils une formation sur l'utilisation des supports d'accès ?
- Existe-t-il un programme continu de sensibilisation aux consignes de sécurité et aux comportements à adopter ?
- Les collaborateurs savent-ils comment signaler des activités suspectes ?

10. Pérennité et développement

- Notre solution d'accès est-elle évolutive pour s'adapter à de nouveaux sites ou à des exigences supplémentaires ?
- Pouvons-nous intégrer sans difficulté les nouvelles normes de sécurité (mises à jour NIS2, directives du BSI, extensions de la loi-cadre KRITIS) ?
- Disposons-nous d'un plan de modernisation clair au cas où certaines technologies deviendraient obsolètes ou que des failles de sécurité seraient découvertes ?

Les directives NIS2 et CER sont transposées dans les différents États membres de l'UE sous les appellations juridiques nationales suivantes :

	NIS2	CER
Autriche	NISG2026 (Loi de 2026 sur la sécurité des réseaux et de l'information)	RKEG (Loi sur la résilience des infrastructures critiques)
Allemagne	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Loi visant à renforcer la résilience physique des infrastructures critiques)
Belgique	Loi NIS2 (Loi du 26 avril 2024 relative à la cybersécurité des réseaux et des systèmes d'information)	Loi relative à la résilience des entités critiques (loi nationale de transposition de la directive CER, 2025/26)
Pays-Bas	Cyberbeveiligingswet (en cours de transposition législative, situation en avril 2026)	Wet weerbaarheid kritieke entiteiten (projet de loi sur les CER, situation en avril 2026)
Suède	Cybersäkerhetslagen (Loi sur la cybersécurité, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (Mise en œuvre de la CER en cours de préparation, situation en avril 2026)
Italie	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Tschechien	Zákon o kybernetické bezpečnosti (Amendement/nouvelle version relative à la transposition de la directive NIS2)	Zákon o odolnosti kritických subjektů (Loi de transposition de la CER)
Polen	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) – Amendement à la directive NIS2	Ustawa o odporności podmiotów krytycznych (en cours de mise en œuvre)
Slovaquie	Zákon o kybernetickej bezpečnosti (NIS2-Novelle)	Zákon o odolnosti kritických subjektov

www.evva.com