Atelier

Fonctions CYBER

Matinale BET

Niagara Framework

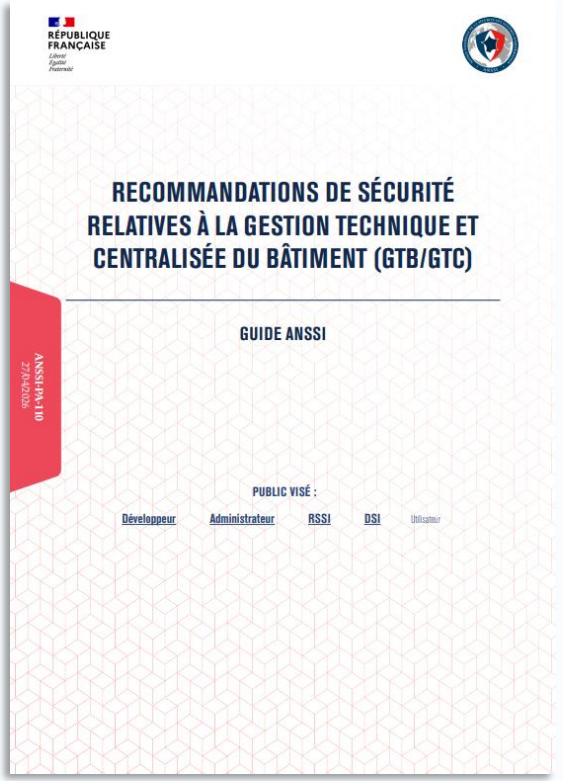
niagara4

ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information

Autorité nationale de référence en matière de cybersécurité et de cyberdéfense en France

- Défendre : Assurer la veille, la détection et la réaction face aux attaques informatiques, notamment pour les services de l'État et les opérateurs d'importance vitale (OIV).
- Connaître : Analyser les menaces, anticiper les modes opératoires des attaquants et comprendre l'évolution du cyberespace
- Partager : Diffuser des alertes, des consignes de sécurité et sensibiliser les entreprises, les administrations et le grand public.
- Accompagner : Offrir son expertise technique, conseiller les autorités et aider à la sécurisation des systèmes numériques.
- Réguler : Définir des règles, qualifier des produits de sécurité et certifier des prestataires de confiance.



Cyber Resilience Act.

- Règlement Européen
- Mise en application en juin 2026
- Exigences de cybersécurité aux produits comportant des éléments numériques
- Devoir d'information des vulnérabilités

S'applique aux entreprises qui mettent sur le marché :

- Fabricants et Editeurs
- Distributeur (au sens CRA)

CRA traite les intégrateurs avec des obligations très limitées, essentiellement le respect des instructions du fabricant et de la configuration prévue.

https://www.entreprises.gouv.fr/decryptages-de-nos-experts/cyber-resilience-act-cra-ce-qui-change-pour-les-entreprises-et-comment

Network and Information Security 2

- Directive Européenne
- Mise en application 2027 (en cours de transposition dans la loi française)

Objectif :

- Garantir la continuité des activités économiques critiques en cas de cyberattaque

Méthode :

- Imposer un socle minimal de cybersécurité à un certain nombre d'acteurs critiques, les opérateurs de service essentiel (OSE) et les fournisseurs de services numériques (FSN)

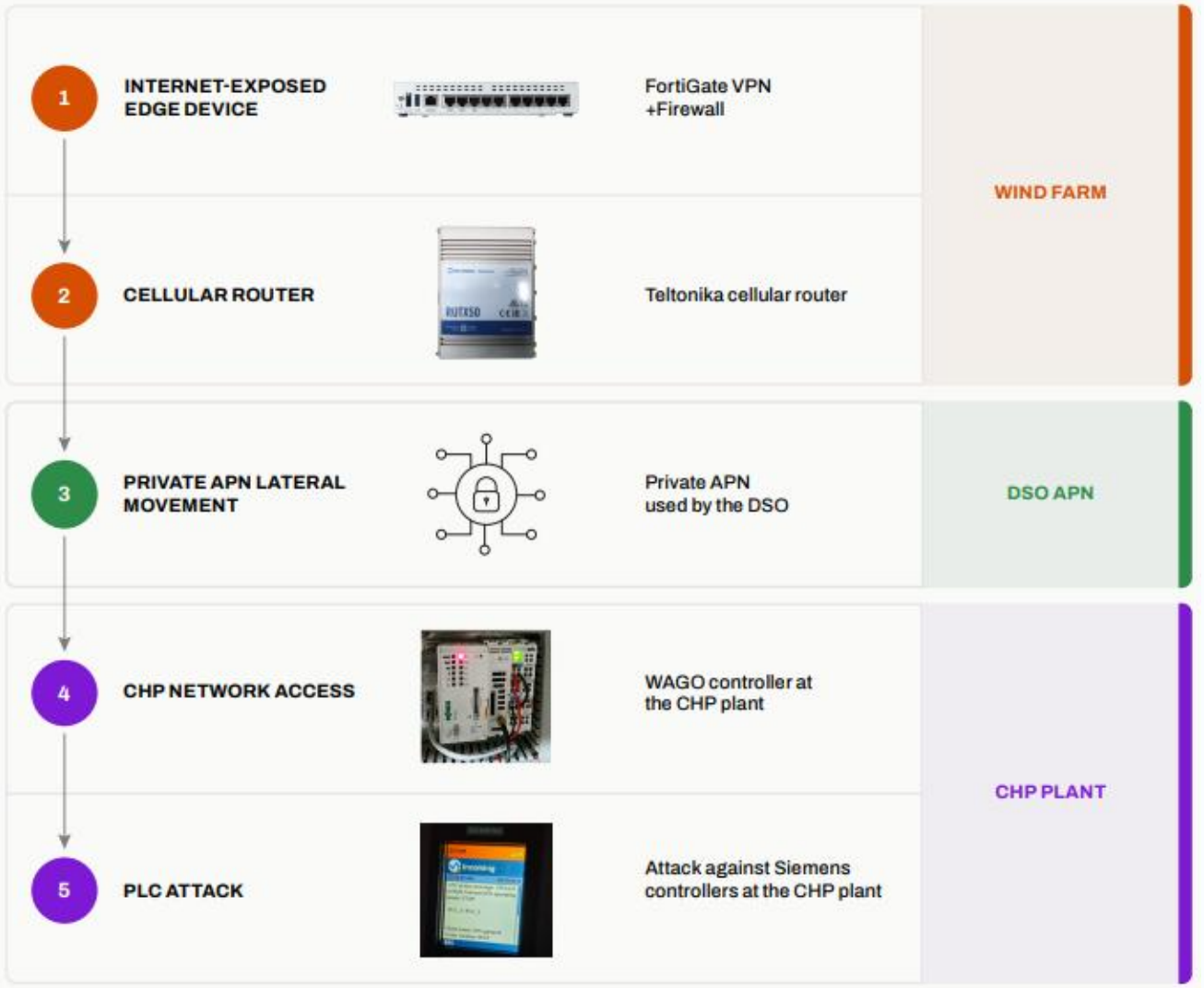
https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/

Pourquoi se protéger ?

Les attaques se multiplient

- Attaque d'une centrale de cogénération en Pologne (Russie ?)

https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Follow_up_Report_2025.pdf



Pourquoi se protéger ?

Les attaques se multiplient

- Attaque d'une centrale de cogénération en Pologne (Russie ?)

https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Follow_up_Report_2025.pdf

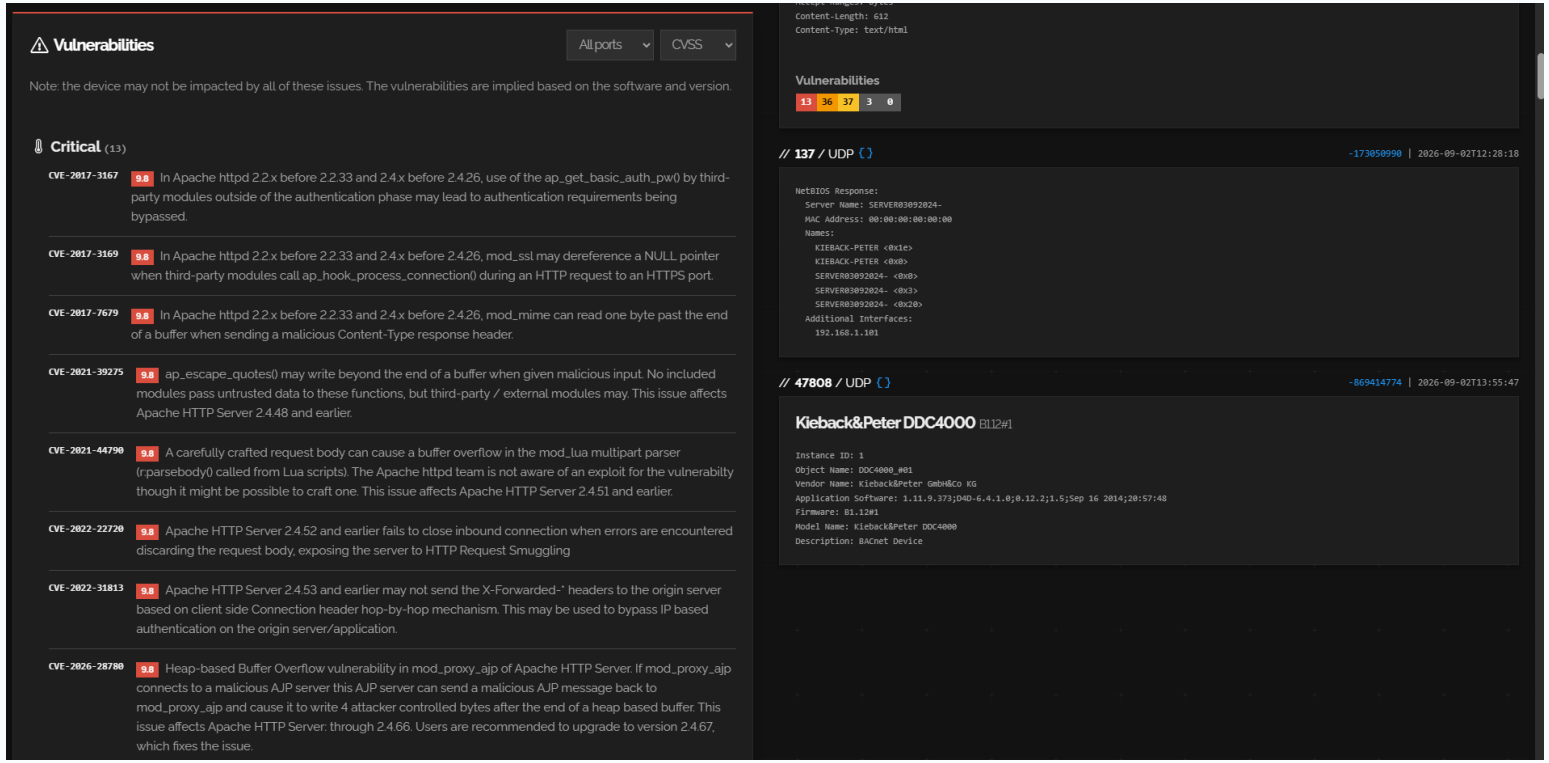
- Attaque de l'industrie US (Iran ?)

https://edition.cnn.com/2026/04/07/politics/iran-linked-hackers-disrupt-us-industrial-sites

Pourquoi se protéger ?

Vous pensez être caché ?

- Moteur de recherche dédié
- Automatisation des attaques (IA)



Pourquoi se protéger ?

Vous pensez être caché ?

- Moteur de recherche dédié
- Automatisation des attaques (IA)

Attention aux certifications

- CSPN (vérifier les versions et le système certifiés)

La faille principale ?

Les logiciels de connexion à distance> A proscrire sur site

La Cybersécurité doit être un pilier du Bâtiment Connecté

- **Les réseau OT sont des cibles faciles**
- **Le secteur est en retard**
- **La législation va accélérer l'adoption du marché**

Pour la Cyber, la prescription et le commissionning vont devenir un impératif !

En détail

Quelques principes

Secure by default / by design

- Par défaut, les sécurités sont activées et maximales
- Par design, certaines actions ou configurations sont impossibles
- Pour amener un haut niveau de sécurité sans hyper spécialistes

Moindre privilège

- Seul ce qui est nécessaire est autorisé, pas plus
- S'applique aux droits d'accès, au cloisonnement réseau, à l'accès physique, etc.
- Pour limiter l'impact d'une faille de sécurité

Défense en profondeur

- Chaque élément et process du SI doit être sécurisé indépendamment
- Pour multiplier les obstacles et éviter de se reposer sur une seule protection

Thématiques NIS2

Recensement des SI	Rôles et responsabilités	Politique de sécurité des systèmes d'information	Gestion de la conformité	Cartographie de l'écosystème	Sécurité numérique dans les contrats avec les prestataires et fournisseurs informatiques	Sécurité des ressources humaines
Cartographie des systèmes d'information	Maintien en condition opérationnelle et de sécurité	Maîtrise des accès physiques	Cloisonnement	Filtrage des communications	Sécurisation des accès distants	Protection contre les codes malveillants
Identification	Authentification	Droits d'accès	Comptes d'administration	Sécurité des annuaires	Gestion des incidents	Continuité et reprise d'activité
Gestion de crise	Exercices, tests et entraînements	Approche par les risques	Audits de la sécurité	Sécurisation de la configuration	Administration des SI	Supervision de la sécurité

Apport Niagara

Recensement des SI	Rôles et responsabilités	Politique de sécurité des systèmes d'information	Gestion de la conformité	Cartographie de l'écosystème	Sécurité numérique dans les contrats avec les prestataires et fournisseurs informatiques	Sécurité des ressources humaines
Cartographie des systèmes d'information	Maintien en condition opérationnelle et de sécurité	Maîtrise des accès physiques	Cloisonnement	Filtrage des communications	Sécurisation des accès distants	Protection contre les codes malveillants
Identification	Authentification	Droits d'accès	Comptes d'administration	Sécurité des annuaires	Gestion des incidents	Continuité et reprise d'activité
Gestion de crise	Exercices, tests et entraînements	Approche par les risques	Audits de la sécurité	Sécurisation de la configuration	Administration des SI	Supervision de la sécurité

Cartographie des systèmes d'information

Outils

- Bases de données Niagara interrogeables en temps réel
- Exports des équipements repris, des adresses IP, des protocoles et ports utilisés
- Toujours à jour

Maintien en condition opérationnelle et de sécurité

Secure by default / by design

- Niagara est certifié IEC 62443
  (cybersécurité des systèmes d'automatisation et de commande industriels)
  - analyse de code, revue cyber dédiée, audits externes, etc.
- Sécurisation des développements tiers
- Participation active au CERT-US pour la gestion des vulnérabilités et des patchs de sécurité
- Mise à jour continue des algorithmes et technologies utilisés
  - Hachage md5 1 000 fois => Hachage pbkdf2 100 000 fois
  - Chiffrement RSA 1024 bits à 4096 bits, Eliptic Curve P-256 à P-521
  - SSL à TLS 1.3

Outils

- Architecture modulaire du logiciel permettant l'application des patchs et mises à jour sans reprogrammation ou perte

Maîtrise des accès physiques

Le fait de placer les serveurs Niagara dans des locaux protégés ne dépend bien sûr pas de Niagara

Secure by default / by design

- Jace 9000 : par défaut, les ports USB et série sont désactivés ainsi que les communications SSH/SFTP

Outils

- Architecture Web distribuée : mitigation des risques et mise à disposition de simples postes clients plutôt que de placer le serveur dans des emplacements risqués
- Les contrôleurs Niagara (JACE, MAC36, etc.) peuvent gérer des protocoles filaires là où l'IP est à éviter

Cloisonnement / Filtrage des communications

Une grande partie de ces thématiques repose sur l'architecture réseau (VLAN, DMZ, Firewall…) dans laquelle Niagara pourra s'intégrer sans problème.

Secure by default / by design

- Contrôleurs Niagara JACE : ports IP disjoints (permet d'isoler des communications IP non chiffrées comme Modbus, Knx, LonWorks, BACnet)
- Support 802.1x et Wi-Fi sécurisé (hardware sans Wi-Fi disponible)
- JACE 9000 : firewall configuré automatiquement intégré
- Communications HTTPS seules activées par défaut (serveur Web, programmation, administration)

Outils

- Support natif de protocoles sécurisés : BACnet/SC, SNMPv3, OPC UA, MQTTS, API HTTPS
- Également pour l'ensemble des communications : mails, SFTP, SSH, bases de données SQL, connecteurs, LDAP/SAML, Syslog, etc.

Sécurisation des accès distants

Cette thématique repose sur l'architecture réseau dans laquelle Niagara pourra s'intégrer sans problème.

Outils

- Niagara Remote : accès distant sécurisé et isolé sans installation supplémentaire
- Niagara Data Service : accès sécurisé aux données du site par API
- Contrôleurs MAC36 : VPN WireGuard intégré

Protection contre les codes malveillants

Secure by default / by design

- Boot sécurisé
- Modules signés : pour empêcher leur altération
- Protection contre l'injection de code
- Content Security Policy (CSP) pour l'interface Web
- Protections Host, XSS, DDOS, etc.

Outils

- Les CSP et protections Web sont personnalisables pour s'adapter au mieux

Identification / Authentification

Secure by default / by design

- Par de mot de passe par défaut
- Pas de compte public : obligation de se connecter
- Authentification forte : SCRAM-SHA256 (les mots de passe ne transitent jamais)
- Politique sur les mots de passe par défaut : dureté, renouvellement, réutilisation
- Politique de déconnexion automatique
- Protection attaque en force brute

Outils

- Configuration des politiques ci-dessus personnalisable
- Mise en place MFA : en consultation comme en édition
- Authentification par certificat client : écrans tactiles ou logiciels par exemple
- Possibilité de créer des comptes temporaires
- Plusieurs types d'authentification peuvent cohabiter (cf. plus loin LDAP / SSO)

Droits d'accès

Secure by default / by design

- Droits sur la consultation, l'édition et l'administration des hôtes séparés
- Fonctions critiques définies par défaut dans une catégorie de droits dédiée
- L'ensemble des propriétés et vues ont un paramétrage prédéfini

Outils

- L'ensemble de ce paramétrage est personnalisable pour appliquer finement le principe du moindre privilège
- Gestion RBAC (Role Based Access Control) complète :
  - création des utilisateurs (comptes nominatifs),
  - rôles (pour faciliter l'administration des droits),
  - catégories de sécurité (pour différentier l'application des droits)
- Permet également de déléguer la gestion des droits utilisateurs (LDAP /Active Directory par exemple)

Gestion des incidents / Continuité et reprise d'activité

Secure by default / by design

- Journalisation automatique
  - Erreurs
  - Connexions
  - Modifications
- Pour permettre une meilleure analyse des incidents de sécurité

Outils

- La mise en place du MFA sur des comptes nominatifs améliore grandement cette analyse
- Backups automatiques y compris sur le Cloud de façon sécurisée (Niagara Recover)
- Possibilité d'installer Niagara en Docker avec une licence par souscription pour les architectures haute disponibilité / haute fiabilité
- Ces deux derniers points facilitant grandement la reprise d'activité en cas de sinistre

Sécurisation de la configuration

Secure by default / by design

- Installation propre et sécurisée de Niagara
  - Isolement des différentes fonctions (exécution du service, édition, administration Niagara)
  - Cloisonnement strict entre la partie serveur Web et l'hôte
- Protection à froid des données sensibles dans la sauvegarde

Administration des SI

Secure by default / by design

- Pour les communications sécurisées par défaut : certificat par serveur auto-signé
- Attention : insuffisant seul

Outils

- Gestion des certificats complète
  - Définition des usages, SAN, révocation de certificat
  - Signature de certificats par des tiers (autorité locale ou publique, chaînes)
  - Bonus : interface plus rapide en plus d'être plus sécurisée
- Gestion centralisée pour améliorer la sécurité et faciliter son déploiement
  - Déploiement massif
  - Signature automatique
  - Alertes sur les expirations (certificats, SMA…)
  - Centralisation de la gestion des utilisateurs (LDAP / SSO par SAML 2)
- Outils tiers DSI, pur Niagara ou hybride

Supervision de la sécurité

Secure by default / by design

- Dashboard sécurité automatique : pour analyser/auditer la posture de sécurité

Outils

- Intégration du SI Niagara/GTB dans les outils de la DSI
  - SNMP
  - Syslog pour connexion à un SIEM (Security Information and Event Management)

BTIB

Connecting Buildings

commercial@btib.fr