EIWTC · CER / NIS-2 / CRA

Transcription du podcast

Cyber- und Sabotageschutz im Wasserwerk

Français – traduction de la version allemande révisée

Traduction d’une version écrite allemande révisée sur la base du PDF fourni ; aucune vérification mot à mot avec l’audio. Informations spécialisées, pas de conseil juridique.

Sommaire

01 · Accueil, enjeux et présentation du cadre
02 · Hypothèses du modèle et approche « tous risques »
03 · Stratégie nationale et articulation entre CER, NIS 2 et CRA
04 · Lois du 5 mai 2026, articles applicables et responsabilités
05 · Couches de protection et cycle de vie des droits d’accès
06 · Limites des serrures mécaniques, état de la technique et maturité
07 · Architecture du système, cryptographie et rôle du CRA
08 · Analyse détaillée des trois cas pratiques d’audit
09 · Notifications et autorités compétentes : 24 h, 72 h, un mois
10 · Plan de mise en œuvre sur 90 jours et quatre décisions de direction
11 · Approfondissements : DORA, règles particulières et aspects techniques

Chapitre 1: Accueil, enjeux et présentation du cadre

Animateur (Chris)
Bienvenue dans cet épisode spécial de notre podcast consacré aux infrastructures critiques et à la résilience ! Nous abordons aujourd'hui un sujet qui paraît, au premier abord, très concret et quotidien, mais qui constitue, à y regarder de plus près, un lien direct entre la cybersécurité, la protection physique contre le sabotage et la réglementation publique : le contrôle d'accès aux infrastructures critiques, à travers l'exemple d'une usine de traitement de l'eau.

Klaus Wollscheid
Bonjour Chris, merci beaucoup de m'avoir invité ! Je suis ravi d'être ici. En tant que CEO d'EIWTC SARL et CSO de BEWENG S.A., je travaille tous les jours précisément à cette interface. Qu'il s'agisse d'une usine d'eau potable, d'un hôpital ou d'un centre de données, une porte ouverte sans autorisation peut, dans le pire des cas, paralyser tout un service essentiel.

Animateur (Chris)
Klaus, nous avons un programme particulièrement dense aujourd'hui. Depuis les nouvelles lois luxembourgeoises du 5 mai 2026, qui ont transposé en droit national les directives européennes CER et NIS 2, et avec le règlement européen sur la cyberrésilience, le CRA, les exploitants font face à des obligations juridiques et techniques très concrètes. Nous voulons explorer chaque détail : du principe des couches de protection au cycle de vie des droits d'accès, en passant par des cas pratiques d'audit et les règles particulières des diapositives complémentaires.

Klaus Wollscheid
Absolument ! Le plus important, c'est que nous ne resterons pas dans l'abstraction. Nous prendrons pour fil conducteur un modèle très parlant : notre usine d'eau potable critique, fictive mais tout à fait réaliste. Car, dans une telle installation, l'enjeu n'est rien de moins que la continuité de l'approvisionnement de la population en eau potable.

Chapitre 2: Hypothèses du modèle et approche « tous risques »

Animateur (Chris)
Commençons directement par cette usine. Quels sites et quelles zones notre exemple comprend-il exactement ?

Klaus Wollscheid
Pour notre modèle, nous supposons que l'usine a été officiellement désignée comme entité critique. Elle se compose généralement de quatre zones essentielles. Premièrement, le portail extérieur du site, où les visiteurs sont accueillis et accompagnés. Deuxièmement, le bâtiment d'exploitation, dans lequel les techniciens reçoivent des droits liés à leur mission. Troisièmement, le poste de conduite central, où le personnel assure la continuité du service jour et nuit et où les interventions de maintenance nécessitent une autorisation formelle. Quatrièmement, le cœur de l'installation : les équipements de commande et les capteurs. Nous ajoutons une station de pompage décentralisée et éloignée, dont la connexion réseau peut être interrompue par moments.

Animateur (Chris)
C'est un exemple extrêmement concret ! Pourquoi le contrôle d'accès joue-t-il un rôle si déterminant dans cette configuration ? Qu'est-ce qui peut mal tourner ?

Klaus Wollscheid
Dans la gestion moderne de la sécurité, nous parlons de l'approche « tous risques », ou all-hazards : les risques physiques et numériques doivent être examinés ensemble. Prenons une chaîne d'événements. Un badge de salarié perdu ou volé reste valide dans le système. Une personne non autorisée l'utilise pour franchir une porte. Elle accède à une armoire de commande ou à une prise réseau accessible dans le bâtiment d'exploitation. Elle y effectue une manipulation ou introduit un logiciel malveillant : le système de commande tombe brusquement en panne et l'alimentation en eau potable est perturbée ! Une porte insuffisamment protégée peut donc provoquer directement un incident informatique et l'interruption du service.

Animateur (Chris)
Et l'approche « tous risques » va bien au-delà du sabotage classique, n'est-ce pas ?

Klaus Wollscheid
Exactement. En plus des cyberattaques et du sabotage intentionnel, nous évaluons toujours les risques naturels, comme les inondations, mais aussi les coupures de courant, l'absence de personnel lors de pandémies et les difficultés d'approvisionnement. Il faut tout examiner conjointement : voies d'accès, dépendances, conséquences et plans concrets de redémarrage.

Chapitre 3: Stratégie nationale et articulation entre CER, NIS 2 et CRA

Animateur (Chris)
Cela nous amène au cadre juridique et stratégique. Le Luxembourg s'est doté d'une stratégie nationale de résilience fondée sur huit piliers. Comment ces textes s'y inscrivent-ils ?

Klaus Wollscheid
Le Luxembourg organise sa résilience autour de huit piliers : pilier 1, la démocratie, l'État de droit et le gouvernement ; pilier 2, une société résiliente ; pilier 3, celui de CER, les services essentiels et les infrastructures critiques ; pilier 4, une économie résiliente ; pilier 5, les ressources stratégiques et logistiques ; pilier 6, celui de NIS 2, la cyberrésilience ; pilier 7, la défense civile ; et pilier 8, la protection et la défense du territoire national. La distinction apparaît clairement : CER protège la continuité physique et opérationnelle des services, NIS 2 protège les réseaux et systèmes numériques, et le Cyber Resilience Act, ou CRA, renforce la sécurité des produits numériques utilisés.

Animateur (Chris)
Quels secteurs sont concernés par ces cadres réglementaires au Luxembourg ?

Klaus Wollscheid
CER couvre douze secteurs : énergie, transports, banques, infrastructures des marchés financiers, santé, eau potable, eaux usées, infrastructures numériques, administration publique, espace, alimentation et gestion des déchets. NIS 2 recouvre nombre de ces domaines et comprend également d’autres secteurs, notamment : les services TIC destinés aux entreprises, les services postaux et de messagerie, les produits chimiques, certaines industries manufacturières, les fournisseurs numériques et la recherche. Ce panorama des secteurs est simplifié : l’assujettissement dépend du type d’entité, des critères de taille et des dispositions particulières prévues par la loi.

Animateur (Chris)
Comment classe-t-on les organisations de ces secteurs ? On entend parler d'entités « critiques », « essentielles » et « importantes ».

Klaus Wollscheid
C'est un point absolument décisif dans les audits ! Sous CER, il s'agit de la catégorie des « entités critiques », désignées officiellement par l'État en raison de leur importance pour la société. NIS 2 distingue les « entités essentielles », généralement les grandes organisations de l'annexe I ou celles relevant de dispositions particulières, et les « entités importantes », notamment les entreprises moyennes de l'annexe I ainsi que les entreprises moyennes et grandes de l'annexe II. Pour notre usine d'eau, un principe important s'applique : dès qu'elle est officiellement désignée comme critique sous CER, elle relève automatiquement de la catégorie des « entités essentielles » sous NIS 2, quels que soient ses effectifs ou son chiffre d'affaires !

Chapitre 4: Lois du 5 mai 2026, articles applicables et responsabilités

Animateur (Chris)
Passons aux bases légales luxembourgeoises. Quelle date les responsables de la sécurité doivent-ils entourer en rouge dans leur calendrier ?

Klaus Wollscheid
Le 5 mai 2026 ! C'est à cette date qu'ont été publiées au Mémorial A les deux lois nationales : le numéro A 225 concerne NIS 2 au Luxembourg et le numéro A 226 concerne CER. Ces deux lois sont entrées en vigueur le 10 mai 2026. Et fait remarquable : elles placent toutes deux les mesures de sécurité sous le même numéro d'article, l'article 12 !

Animateur (Chris)
À quels endroits l'article 12 de la loi CER et l'article 12 de la loi NIS 2 relient-ils ces obligations au contrôle d'accès ?

Klaus Wollscheid
Dans la loi luxembourgeoise CER, l'article 12, paragraphe 1, points 2 et 5, correspondant à l'article 13, paragraphe 1, points b et e, de la directive européenne CER, impose une protection physique des installations ainsi que des mesures adaptées de sécurité du personnel et de gestion des autorisations d'accès. Dans la loi luxembourgeoise NIS 2, l'article 12, paragraphe 2, points 8 à 10, correspondant à l'article 21, paragraphe 2, points h, i et j, de la directive européenne NIS 2, traite de la cryptographie, du contrôle strict des accès, de la sécurisation des accès physiques et d'une authentification appropriée. Dans notre usine, cela signifie concrètement que seules les personnes autorisées entrent au poste de conduite, que le serveur de contrôle d'accès est renforcé sur le plan numérique, que les droits retirés deviennent effectivement inopérants dans le délai fixé selon les risques et que le fonctionnement en mode dégradé a été testé.

Animateur (Chris)
Qu'en est-il de la responsabilité de la direction et des sanctions encourues ?

Klaus Wollscheid
La direction assume des obligations précises en matière de sécurité ! Sous NIS 2, la formule est la suivante : approuver, rendre possible, surveiller et apprendre. La direction doit approuver le concept de contrôle d'accès, dégager les budgets et les ressources, superviser les essais de panne et tirer les enseignements des écarts. En cas de manquement répondant aux conditions légales, NIS 2 prévoit pour les entités des amendes pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial pour les entités essentielles, et 7 millions d'euros ou 1,4 % pour les entités importantes. Sous CER, l'article 19 national prévoit des amendes pouvant aller jusqu'à 250 000 euros. Ces sanctions visant les entités ne signifient pas automatiquement que chaque dirigeant engage sa responsabilité personnelle ; celle-ci dépend de conditions légales distinctes.

Animateur (Chris)
Quels délais les exploitants et les fabricants doivent-ils respecter ?

Klaus Wollscheid
Reprenons la chronologie. CER et NIS 2 sont entrées en vigueur au Luxembourg le 10 mai 2026. La date limite pour le premier auto-enregistrement NIS 2 était le 10 juillet 2026. Depuis le 11 septembre 2026, les premières obligations de notification prévues par le CRA s'appliquent aux fabricants en cas de vulnérabilités activement exploitées. Le 11 décembre 2027, les principales obligations du règlement européen sur la cyberrésilience, le CRA 2024/2847, entreront en application pour les produits numériques. Pour les entités désignées sous CER, l'analyse approfondie des risques doit en outre être disponible dans les neuf mois suivant la désignation et les dispositions concernées du chapitre 4 deviennent en principe applicables après dix mois, sous réserve des exceptions légales !

Chapitre 5: Couches de protection et cycle de vie des droits d’accès

Animateur (Chris)
Venons-en au cœur de la protection physique : le principe des couches concentriques, souvent appelé « principe de l'oignon ». Comment l'applique-t-on à notre usine d'eau ?

Klaus Wollscheid
Le principe de l'oignon répartit le site en quatre limites de protection imbriquées, de l'extérieur vers l'intérieur. La couche 1 correspond au terrain et au périmètre extérieur : clôture, portail, barrière et gestion des visiteurs. La couche 2 correspond au bâtiment et à son périmètre intérieur : des portes extérieures contrôlées qui n'admettent que les personnes autorisées. La couche 3 englobe les locaux sensibles : poste de conduite, laboratoire ou salle serveurs, chacun doté de droits d'accès propres aux rôles. La couche 4 protège directement les composants critiques : armoire de commande fermée à clé, automate programmable ou baie serveur, dont l'ouverture exige une autorisation spécifique pour une tâche précise. Chaque couche correctement conçue vise à ralentir les accès non autorisés et à permettre une réaction. La norme EN 50600-2-5 concerne les systèmes de protection des centres de données : nos quatre couches sont ici un modèle de planification pour l’usine d’eau, et non une exigence générale de cette norme.

Animateur (Chris)
Comment cela se déroule-t-il concrètement pour un technicien de maintenance externe ?

Klaus Wollscheid
Supposons qu'un technicien externe doive intervenir aujourd'hui sur la pompe 3 au poste de conduite. À la couche 1, au portail, son identité et son rendez-vous sont vérifiés et il reçoit un badge à l'accueil. À la couche 2, à l'entrée du bâtiment, ce badge n'ouvre l'accès que pendant un créneau limité. À la couche 3, au poste de conduite, le responsable d'exploitation autorise l'entrée, éventuellement sous accompagnement. À la couche 4, à l'armoire de commande, la boîte à clés ou le dispositif de déverrouillage de cette armoire précise est activé. À la fin de l’intervention, les droits temporaires sont retirés selon la procédure convenue, les armoires sont refermées et les étapes essentielles sont consignées de manière vérifiable !

Animateur (Chris)
Comment gérer ces autorisations tout au long du parcours des salariés et des entreprises externes ?

Klaus Wollscheid
Nous parlons du cycle de vie des droits d'accès, en trois étapes. Première étape : arrivée, vérification de l'identité, attribution du rôle dans le système RH et remise d'une carte. Deuxième étape : changement de fonction ou de service ; les anciens droits sont retirés de manière effective conformément à la procédure définie et seuls les nouveaux droits nécessaires sont accordés. Troisième étape : départ ; le badge doit devenir inutilisable dans le délai défini ; l’effet réel du blocage doit être contrôlé et documenté. Pour certaines fonctions sensibles définies par la loi, une vérification formelle du personnel peut être nécessaire dans le cadre de CER. La décision correspondante est en principe valable cinq ans et le renouvellement doit être demandé dans le délai légal, entre six et quatre mois avant l’expiration !

Animateur (Chris)
Que se passe-t-il lorsqu'une couche est défaillante ou contournée ?

Klaus Wollscheid
C'est le véritable test de résistance ! Si la couche 1, par exemple le portail, reste ouverte à cause d'une panne, les couches intérieures 2, 3 et 4 doivent continuer à limiter efficacement les accès non autorisés. Parallèlement, une situation anormale, comme une porte du poste de conduite ouverte trop longtemps, devrait être détectée par une surveillance adaptée et donner lieu à une réaction définie à l'avance. Les fournisseurs et les accès secondaires doivent être intégrés à des règles d'accès appropriées et clairement documentées.

Chapitre 6: Limites des serrures mécaniques, état de la technique et maturité

Animateur (Chris)
Beaucoup de petites usines ou d'installations anciennes reposent encore sur des serrures purement mécaniques. Pourquoi cela ne suffit-il souvent plus sous NIS 2 et CER ?

Klaus Wollscheid
Les clés purement mécaniques présentent trois faiblesses majeures dans un audit. Premièrement, la traçabilité : une serrure mécanique ne crée pas de journal numérique des événements ; elle ne permet pas à elle seule de savoir qui a ouvert la porte et quand. Deuxièmement, la perte et les copies : si un passe général est perdu, il ne peut pas être bloqué d'un clic, et il faut évaluer, selon la hiérarchie du plan de fermeture, les cylindres concernés et les mesures de remplacement adaptées. Troisièmement, la gestion du temps et des rôles : une clé mécanique fonctionne à toute heure et ne connaît ni les horaires de travail ni les fenêtres temporaires de maintenance.

Animateur (Chris)
NIS 2 demande des mesures correspondant à l'« état de la technique ». Comment comprend-on cette notion juridique dans le contexte du contrôle d'accès ?

Klaus Wollscheid
L'état de la technique désigne des mesures de protection correspondant au développement technologique actuel, adaptées au risque considéré et réellement efficaces. Le processus comporte quatre étapes : déterminer les risques et les besoins de protection ; sélectionner des mesures appropriées sur la base de normes ; tester et démontrer leur efficacité en exploitation ; puis les réévaluer régulièrement. L'effort et les coûts entrent en compte dans la proportionnalité, mais le niveau de protection nécessaire de l'installation critique demeure déterminant !

Animateur (Chris)
Vous avez également élaboré un modèle de développement très parlant, en quatre niveaux. Peux-tu nous expliquer ces degrés de maturité ?

Klaus Wollscheid
Volontiers. Niveau 01, réactif/mécanique : clés purement mécaniques, remise consignée manuellement et remplacement éventuel de la serrure en cas de perte. Niveau 02, identifié/électronique : équipements électroniques et identifiants RFID ; les badges individuels permettent des journaux d'événements et le blocage ciblé d'une carte, même si le délai effectif dépend fortement de l'architecture. Niveau 03, dynamique/gestion des droits : gestion des rôles et autorisations automatisée selon les capacités du système, créneaux de maintenance limités et lien automatique avec le système RH lors d'un départ. Niveau 04, proactif/surveillance : supervision ciblée des accès sensibles selon le risque, éventuellement avec détection automatisée d'attaques, authentification multifacteur adaptée au risque, par exemple carte et code PIN au poste de conduite, et essais réguliers du mode dégradé.

Chapitre 7: Architecture du système, cryptographie et rôle du CRA

Animateur (Chris)
Lorsque nous installons un système électronique de contrôle d'accès, ce système devient lui-même une cible intéressante pour les cyberattaques. Comment protéger son infrastructure ?

Klaus Wollscheid
Précisément pour cette raison, le système de contrôle d'accès doit lui aussi être renforcé ! La chaîne comprend le badge, le lecteur, le contrôleur de porte et le logiciel de gestion. Selon les besoins de protection, des contacts anti-sabotage et des dispositifs de verrouillage adaptés peuvent être nécessaires sur la porte. Le serveur de contrôle d’accès doit être sécurisé selon l’analyse des risques, notamment, lorsque c’est approprié, par une segmentation réseau et une authentification multifacteur de l’administration. Enfin, les communications entre composants requièrent une authentification et des protections cryptographiques adaptées !

Animateur (Chris)
Concrètement, à quoi ressemble cette cryptographie sur les trois liaisons de transmission ?

Klaus Wollscheid
Nous protégeons trois segments. Liaison 1, badge-lecteur : vérifier l'authenticité du badge grâce à des mécanismes chiffrés de type défi-réponse, par exemple MIFARE DESFire, pour limiter efficacement les risques de copie et d’attaques par rejeu. Liaison 2, lecteur-contrôleur : authentifier les messages et protéger le câble de bus contre les manipulations, par exemple avec OSDP v2 Secure Channel. Liaison 3, contrôleur-serveur : vérification mutuelle des certificats et transmission réseau chiffrée. Point essentiel pour les audits : il n'existe pas d'obligation absolue d'utiliser AES-256 ou TLS 1.3 sur chaque porte ; la méthode doit être choisie en fonction du risque et intégrée au cycle de vie de la gestion des clés cryptographiques !

Animateur (Chris)
Quel rôle joue ici le nouveau règlement européen sur la cyberrésilience, le CRA ?

Klaus Wollscheid
Le CRA, règlement (UE) 2024/2847, impose des obligations aux fabricants de produits. Pour les produits relevant du CRA, les fabricants de lecteurs, de contrôleurs et de logiciels de gestion des accès doivent prévoir des paramètres sûrs par défaut, traiter les vulnérabilités pendant la période de support applicable et proposer des mises à jour de sécurité. Le CRA prévoit en principe une durée de support d’au moins cinq ans, sauf si la durée d’utilisation attendue est plus courte ; une utilisation attendue plus longue peut exiger un support prolongé. Lors de la remise du produit, les achats font le lien entre le fabricant et l'exploitant : l'exploitant prend en charge la configuration sécurisée et le fabricant assure les modalités de support et de mise à jour exigées par la loi et convenues contractuellement.

Chapitre 8: Analyse détaillée des trois cas pratiques d’audit

Animateur (Chris)
Nous arrivons à la partie la plus passionnante pour les auditeurs et les professionnels de la sécurité : trois cas pratiques d'audit dans notre usine d'eau ! Commençons par le premier : un salarié perd son badge. Que se passe-t-il ?

Klaus Wollscheid
Le premier cas montre la différence entre une porte en ligne et une porte hors ligne ! Le salarié signale la perte et son badge est bloqué dans le système central. À la porte en ligne du poste de conduite, le blocage peut prendre effet rapidement si la communication fonctionne. Il faut néanmoins vérifier que le contrôleur a reçu la modification et que la porte refuse réellement le badge bloqué. Mais à la porte hors ligne de la station de pompage éloignée, le contrôleur n'est pas connecté en permanence. L'efficacité du blocage y dépend notamment de la mise à jour locale des données de révocation ou de l'expiration d'un droit limité dans le temps. Pour l'audit, cela signifie que le délai maximal de révocation doit être fixé à l'avance dans l'analyse des risques et démontré sur la serrure réelle, y compris lors d'une panne réseau simulée !

Animateur (Chris)
Que montre le deuxième cas : une panne totale de courant ou de réseau dans l'usine d'eau ?

Klaus Wollscheid
Le deuxième cas concerne le fonctionnement en mode dégradé ! Si la connexion réseau tombe en panne, les contrôleurs de porte ne doivent pas ouvrir toutes les portes sans autorisation. Ils doivent continuer à fonctionner en sécurité avec les droits et règles enregistrés localement, conformément à leur conception. En cas de coupure électrique, l'autonomie nécessaire ou une procédure de remplacement appropriée doit être prévue. Il faut surtout coordonner et tester, pour chaque porte, l'évacuation, la protection contre l'accès non autorisé et l'ouverture de secours selon les règles de construction et de sécurité incendie applicables. Le personnel d'exploitation habilité doit cependant pouvoir accéder à l'installation par des voies de secours définies. Lorsque le courant revient, les événements et horodatages doivent être réconciliés de manière contrôlée.

Animateur (Chris)
Et le troisième cas associe ces situations dans un exercice commun de panne. Comment se déroule ce test de résistance ?

Klaus Wollscheid
Nous simulons trois phases pendant l'exercice d'audit. À 08 h 10, le réseau tombe en panne : un technicien doit atteindre le poste de conduite ; l'accès de secours est vérifié et les fonctions d'évacuation prévues sont démontrées. À 08 h 20, un salarié signale la perte de son badge ; le droit est encore enregistré sur l'identifiant de la station de pompage hors ligne ; des mesures organisationnelles de repli prédéfinies limitent efficacement le risque résiduel. À 08 h 35, le système revient : les événements conservés localement sont rapprochés de manière contrôlée dans les limites du système. En cas d'indice de défaut du produit, le fabricant est associé à l'analyse ; l'existence d'une obligation de notification CRA est examinée séparément par l'acteur concerné. Cet exercice fournit des preuves utiles de la résilience opérationnelle !

Chapitre 9: Notifications et autorités compétentes : 24 h, 72 h, un mois

Animateur (Chris)
Lorsqu'un incident grave survient, par exemple un sabotage du contrôle d'accès perturbant l'usine d'eau, des obligations légales strictes de notification peuvent s'appliquer. Comment les voies de notification diffèrent-elles entre NIS 2, CER et CRA ?

Klaus Wollscheid
C'est l'une des questions les plus complexes en pratique, car un seul incident peut déclencher simultanément deux voies de notification légales distinctes ! Regardons les délais. Sous NIS 2, pour les incidents de sécurité importants : premièrement, une alerte précoce dans les 24 heures après en avoir pris connaissance ; deuxièmement, la notification de l'incident dans les 72 heures ; troisièmement, un rapport final obligatoire un mois après la notification. Sous CER, pour les perturbations importantes de la résilience : premièrement, un premier signalement dans les 24 heures après en avoir pris connaissance ; deuxièmement, un rapport final détaillé dans un délai d'un mois. CER ne prévoit pas d'étape intermédiaire générale à 72 heures ! Pour CER, l'autorité compétente est le Haut-Commissariat à la Protection Nationale (HCPN) ; pour NIS 2, il s'agit de l'ILR, ou de la CSSF dans le secteur financier. Les notifications des fabricants liées aux vulnérabilités sous CRA passent par des voies distinctes impliquant l'ENISA et les CSIRT nationaux.

Chapitre 10: Plan de mise en œuvre sur 90 jours et quatre décisions de direction

Animateur (Chris)
Comment intégrer durablement toutes ces exigences dans le système de management de la sécurité de l'information, le SMSI ou ISMS ?

Klaus Wollscheid
Nous recommandons un cycle ISMS fermé, en quatre étapes : identifier le risque, définir la mesure, produire la preuve de son efficacité en exploitation, puis améliorer continuellement. Dans un audit, la documentation compte : plan des zones, revue des droits d'accès, justificatifs de configuration, registres de maintenance, journaux d'incident et procès-verbaux des exercices de secours. Une maturité bien documentée facilite considérablement la supervision, mais elle n'offre aucune dispense automatique d'audit !

Animateur (Chris)
Pour les exploitants qui doivent démarrer maintenant, à quoi ressemble un plan pragmatique de mise en œuvre sur 90 jours ?

Klaus Wollscheid
Nous répartissons les 90 premiers jours en trois phases de 30 jours. Jours 01 à 30, situer et inventorier : vérifier l'applicabilité et l'enregistrement, recenser zones, installations et prestataires, consolider les inventaires des clés et des droits. Jours 31 à 60, combler les lacunes : réaliser l'analyse des risques, définir les priorités, sélectionner des solutions de contrôle d'accès et des processus de révocation appropriés, prévoir les accès de secours et obtenir les engagements des fabricants au titre du CRA. Jours 61 à 90, tester et ancrer : réaliser les essais de panne et de redémarrage sur les portes réelles, former le personnel, constituer le dossier de preuves et intégrer le système dans l'ISMS.

Animateur (Chris)
Pour conclure cette partie principale, quelles sont les quatre décisions essentielles que la direction doit prendre maintenant ?

Klaus Wollscheid
Il y a exactement quatre décisions. Premièrement, confirmer les besoins de protection : fixer des exigences contraignantes pour l'approvisionnement en eau potable, les zones et les durées maximales d'interruption tolérables. Deuxièmement, relier les responsabilités : réunir direction, exploitation, informatique, ressources humaines et fournisseurs externes. Troisièmement, approuver le concept de contrôle d'accès : allouer les budgets nécessaires à la révocation des droits, au mode dégradé, à la cryptographie et au support fabricant. Quatrièmement, démontrer l'efficacité : programmer un exercice commun de panne et évaluer les preuves dans le cadre de l'audit. CER et NIS 2 guident le programme, tandis que le CRA renforce les produits utilisés pour sa mise en œuvre !

Chapitre 11: Approfondissements : DORA, règles particulières et aspects techniques

Animateur (Chris)
Klaus, notre présentation comprend aussi douze diapositives complémentaires riches en informations spécialisées. Explorons les points essentiels pour les experts. Quel est le rapport entre NIS 2, le secteur financier et DORA ?

Klaus Wollscheid
La diapositive complémentaire R4 l'explique clairement. Pour les entités financières concernées, DORA peut s’appliquer en tant que réglementation spéciale ; les éventuels recoupements avec NIS 2 doivent être analysés obligation par obligation. La CSSF supervise les domaines financiers relevant de sa compétence légale. Les attributions au titre de CER et de NIS 2 dépendent du régime et de l’entité, notamment pour le HCPN et l’ILR.

Animateur (Chris)
Comment le CRA distingue-t-il les catégories de produits pour les systèmes de contrôle d'accès ?

Klaus Wollscheid
La diapositive complémentaire R6 présente trois groupes. Catégorie 01, catégorie de base : produits numériques généraux. Catégorie 02, produits importants selon l'annexe III, classes I et II : notamment certains produits de gestion des identités et des accès privilégiés, IAM/PAM, ainsi que certaines serrures connectées ou de sécurité domestique. Catégorie 03, produits critiques selon l'annexe IV : composants spécifiques particulièrement critiques. Point important : un produit ne devient pas un produit critique au sens du CRA simplement parce qu'il est installé dans une infrastructure critique ; sa fonction essentielle détermine son classement !

Animateur (Chris)
Quels critères EIWTC recommande-t-elle pour la réception technique d'un système de contrôle d'accès ?

Klaus Wollscheid
La diapositive complémentaire R7 propose une liste de contrôle en cinq points. Premièrement, identité et autorisation : identification univoque des équipements et essai de blocage concluant. Deuxièmement, communication protégée : liaisons bus et réseau authentifiées et chiffrées. Troisièmement, firmware et mises à jour : micrologiciel signé et essai négatif réussi avec une mise à jour non autorisée. Quatrièmement, clés et certificats : cycle de vie maîtrisé pour le renouvellement, la révocation et le remplacement d'urgence. Cinquièmement, disponibilité et assistance : fonctionnement de secours démontré et un engagement écrit de support fabricant pour la durée pertinente selon le CRA et l’utilisation attendue.

Animateur (Chris)
Quel rôle joue la défense civile et militaire dans le cadre de la stratégie nationale de résilience, la SNR ?

Klaus Wollscheid
La diapositive complémentaire R9 souligne que la résilience nationale exige des responsabilités coordonnées ! Le cadre stratégique national de résilience prévoit des responsables de la résilience et des plans de continuité dans toutes les institutions publiques. Une usine d’eau peut jouer un rôle essentiel dans la continuité des services nationaux et, selon ses missions effectives, dans certaines préparations de crise de l’État. Les contacts et plans de rétablissement sont donc à coordonner avec les autorités compétentes en fonction des responsabilités réellement définies.

Animateur (Chris)
Klaus, c'était un voyage extraordinaire, complet et détaillé à travers toutes les facettes de la cybersécurité et de la protection contre le sabotage des infrastructures critiques ! Merci beaucoup pour cette expertise et ces conseils pratiques.

Klaus Wollscheid
Avec grand plaisir, Chris ! Merci à toi et bonne réussite à tous les exploitants dans la mise en œuvre !