AYI NEDJIMI Consultants

PRA/PCA Cyber : Plan de Reprise et Continuité d'Activité

Catégorie : Conformité Lecture : 14 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet PRA/PCA Cyber : Business Impact Analysis, RTO/RPO, stratégie backup 3-2-1-1-0, reconstruction AD, communication de crise, exercices de.

2.1 Définitions et périmètres

La confusion entre PRA, PCA et PSI est fréquente et source d'erreurs stratégiques. Chaque plan répond à un objectif distinct et s'inscrit dans un continuum de résilience : Guide complet PRA/PCA Cyber : Business Impact Analysis, RTO/RPO, stratégie backup 3-2-1-1-0, reconstruction AD, communication de crise, exercices de. Le cadre réglementaire européen impose des exigences croissantes aux organisations. Ce guide sur pra pca cyber plan reprise fournit les clés de compréhension et de mise en conformité. Nous abordons notamment : 4. scénarios cyber majeurs à intégrer dans le pra, 5. stratégie de sauvegarde 3-2-1-1-0 : le bouclier ultime et 6. reconstruction active directory : procédure de référence. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Plan	Objectif principal	Temporalité	Déclencheur
PCA (Plan de Continuité d'Activité)	Maintenir les activités critiques *pendant* l'incident	Immédiat à court terme (heures/jours)	Tout événement perturbateur
PRA (Plan de Reprise d'Activité)	Restaurer les activités *après* l'incident	Moyen terme (jours/semaines)	Incident majeur avec interruption
PSI (Plan de Secours Informatique)	Reconstruire l'infrastructure IT	Variable selon la complexité	Sinistre impactant le SI
PCO (Plan de Continuité des Opérations)	Maintenir les opérations métier en mode dégradé	Pendant la phase de reconstruction	Activation du PRA/PCA

Le **PCA** est le plan-cadre qui englobe l'ensemble de la stratégie de résilience. Il décrit comment l'organisation maintient ses activités critiques à un niveau acceptable pendant et après un événement perturbateur. Le PCA inclut des volets organisationnels (cellule de crise, communication, ressources humaines), logistiques (sites de repli, fournitures) et techniques (PSI/PRA).

Le **PRA**, quant à lui, est spécifiquement focalisé sur la reprise des activités après interruption. Il détaille les procédures de restauration, l'ordre de redémarrage des systèmes, les vérifications d'intégrité et les critères de retour à la normale. Dans un contexte cyber, le PRA doit intégrer une dimension forensique : on ne restaure pas un environnement compromis sans s'assurer que l'attaquant n'y persiste pas.

Le **PSI** est la composante technique du PRA. Il décrit les architectures de secours, les mécanismes de bascule, les procédures de reconstruction et les configurations de référence. Pour les environnements Active Directory, le PSI doit inclure des procédures spécifiques de reconstruction des contrôleurs de domaine, car AD est le socle d'authentification de l'ensemble de l'infrastructure.

2.2 Spécificités du PRA/PCA Cyber par rapport au PRA/PCA classique

Un PRA classique part du principe que l'incident est localisé et que les systèmes de secours sont intègres. Une cyberattaque invalide ces deux hypothèses :

- **Propagation latérale :** Le ransomware se propage à l'ensemble du réseau, y compris les sites de secours connectés. Les réplications de données propagent le chiffrement aux copies secondaires.
- **Compromission des sauvegardes :** Les groupes de ransomware ciblent systématiquement les systèmes de sauvegarde -- suppression des shadow copies, chiffrement des volumes de backup, destruction des bandes accessibles en réseau.
- **Compromission de l'identité :** L'Active Directory compromis signifie que tous les comptes, tous les mots de passe, tous les certificats sont potentiellement sous contrôle de l'attaquant. La restauration d'une sauvegarde AD restaure aussi les backdoors.
- **Persistance :** Les attaquants déploient des mécanismes de persistance (tâches planifiées, services malveillants, comptes dormants) qui survivent à une simple restauration.
- **Incertitude sur le périmètre :** Contrairement à un incendie dont les dégâts sont visibles, le périmètre d'une compromission cyber est souvent inconnu au moment du déclenchement du PRA.
- **Dimension forensique :** Avant de restaurer, il faut comprendre le vecteur d'attaque pour ne pas réintroduire la vulnérabilité exploitée. La chaîne de preuve numérique doit être préservée pour d'éventuelles poursuites judiciaires.

Bonne pratique : le PRA Cyber doit être un document distinct
Ne tentez pas de "patcher" votre PRA classique avec quelques lignes sur le ransomware. Un PRA Cyber est un document autonome avec ses propres procédures, ses propres critères de déclenchement et ses propres exercices. Il s'articule avec le PRA classique mais ne s'y substitue pas.

Notre avis d'expert
La conformité réglementaire est un marathon, pas un sprint. Trop d'organisations traitent la certification comme un projet ponctuel plutôt qu'un processus continu d'amélioration. Sans appropriation par les équipes opérationnelles, le système de management reste un document mort.

3.3 Matrice BIA : modèle pratique

Voici un modèle de matrice BIA adaptée au contexte cyber, que nous utilisons lors de nos missions d'accompagnement :

Processus métier	Applications / Systèmes	Impact financier (par jour)	Impact réglementaire	RTO cible	RPO cible
Authentification / Accès	Active Directory, Entra ID	Blocage total du SI	NIS 2, DORA	4h	0 (réplication)
Production / ERP	SAP, Oracle, bases métier	500K - 2M EUR	Contractuel	8h	1h
Messagerie	Exchange Online, Teams	50K - 200K EUR	RGPD	24h	4h
Paie / RH	SIRH, logiciel de paie	Variable	Code du travail	72h	24h
Site web / e-commerce	CMS, plateforme e-commerce	100K - 1M EUR	Contractuel	4h	15 min

Cas concret
Clearview AI a été condamnée à des amendes cumulées de plus de 50 millions d'euros par plusieurs autorités européennes pour collecte massive de données biométriques sans consentement. Cette affaire a posé les jalons de la régulation de la reconnaissance faciale en Europe et a alimenté le débat sur l'AI Act.

4. Scénarios cyber majeurs à intégrer dans le PRA

4.1 Scénario 1 : Ransomware avec chiffrement généralisé

C'est le scénario le plus fréquent et le plus critique. Un groupe de ransomware obtient un accès initial (phishing, vulnérabilité, accès RDP exposé), effectue une reconnaissance latérale pendant 5 à 15 jours, élève ses privilèges jusqu'au niveau Domain Admin, désactive les sauvegardes accessibles, puis déploie le chiffrement simultanément sur l'ensemble du parc.

Impact PRA : l'ensemble du SI est indisponible. Les contrôleurs de domaine sont chiffrés, ce qui bloque toute authentification. Les serveurs de sauvegarde ont été ciblés. La reconstruction nécessite une approche from scratch avec des sauvegardes offline si elles existent.

4.2 Scénario 2 : Compromission de l'Active Directory

L'attaquant obtient le contrôle complet de l'AD via des techniques comme le Kerberoasting, le DCSync ou l'exploitation de certificats ADCS. Même sans ransomware, cette compromission donne accès à l'intégralité des données de l'organisation.

Impact PRA : tous les comptes, mots de passe et certificats doivent être considérés comme compromis. La reconstruction de l'AD nécessite la création d'une nouvelle forêt, la migration progressive des objets et la rotation de tous les secrets. C'est l'un des scénarios les plus complexes et les plus longs à traiter.

4.3 Scénario 3 : Attaque supply chain

Un fournisseur de logiciel ou un prestataire infogérance est compromis, et l'attaque se propage via une mise à jour empoisonnée ou des accès VPN partagés. Ce scénario est particulièrement difficile à gérer car l'organisation ne contrôle pas le vecteur initial.

Impact PRA : nécessité d'isoler immédiatement les connexions avec le fournisseur compromis, d'identifier tous les systèmes potentiellement affectés et de qualifier l'étendue de la compromission avant toute reprise.

4.4 Scénario 4 : Exfiltration de données avec menace de publication

Le double extorsion est devenu la norme : les attaquants exfiltrent les données avant le chiffrement, menaçant de les publier si la rançon n'est pas payée. Ce scénario impose des obligations de notification (RGPD Article 33 : notification CNIL sous 72h) et impacte fortement la stratégie de communication de crise.

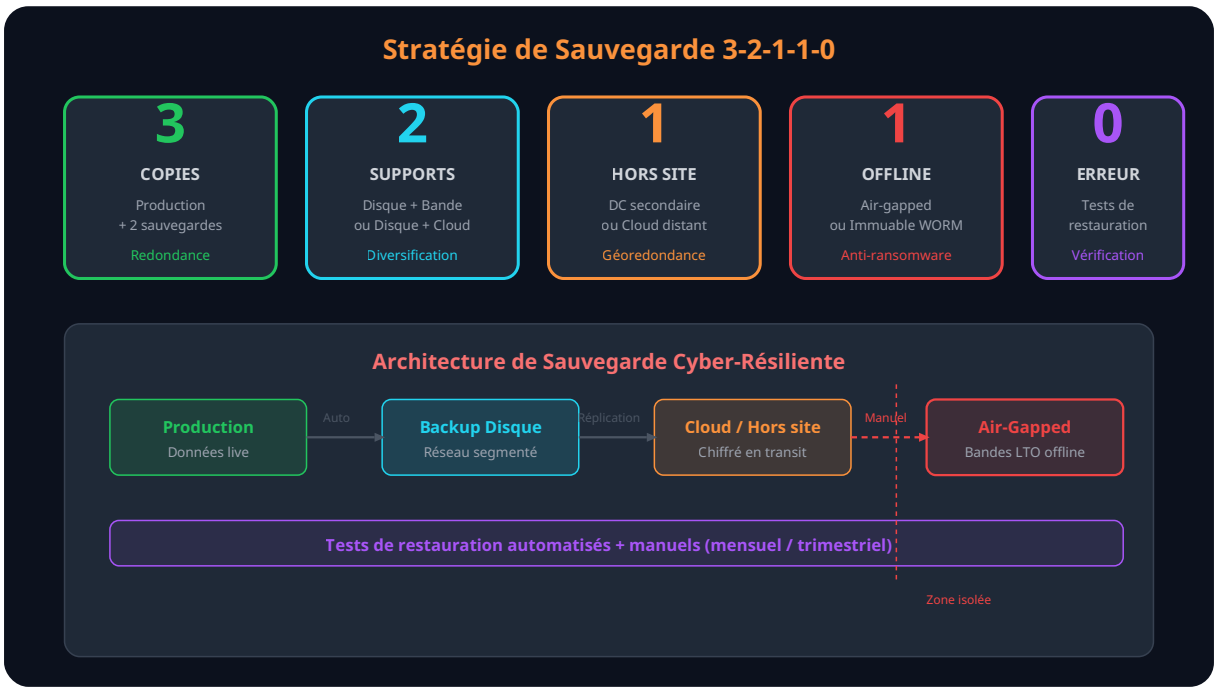
5. Stratégie de sauvegarde 3-2-1-1-0 : le bouclier ultime

5.1 De la règle 3-2-1 à la règle 3-2-1-1-0

La règle de sauvegarde classique **3-2-1** (3 copies, sur 2 supports différents, dont 1 hors site) est insuffisante face aux ransomwares modernes. La règle **3-2-1-1-0** ajoute deux dimensions essentielles :

- **3** copies de chaque donnée
- **2** types de supports différents (disque, bande, cloud)
- **1** copie hors site (datacenter secondaire, cloud)
- **1** copie *offline* ou *air-gapped* (physiquement déconnectée du réseau)
- **0** erreur de restauration vérifiée (tests de restauration réguliers)

Le "1" supplémentaire (copie offline/air-gapped) est le contrôle le plus critique. Un ransomware ne peut pas chiffrer ce qu'il ne peut pas atteindre. Les solutions de stockage immuable (WORM -- Write Once Read Many) constituent une alternative technique à l'air-gap physique, en rendant les données non modifiables pendant une durée définie.



5.2 Sauvegardes Active Directory : le cas critique

La sauvegarde de l'Active Directory mérite une attention particulière car AD est le **pilier fondamental** de l'infrastructure. Sans AD, aucune authentification, aucun accès réseau, aucune application n'est accessible. Les bonnes pratiques de sauvegarde AD incluent :

- **Sauvegarde System State** : inclut la base NTDS.dit, le SYSVOL, le registre et les certificats. À effectuer quotidiennement sur chaque contrôleur de domaine.
- **Sauvegarde bare metal** : image complète du serveur permettant une restauration rapide. Conservation d'au moins 3 générations.
- **Export de la base NTDS.dit offline** : copie de la base AD sur un support déconnecté, chiffrée et stockée en coffre physique.
- **Documentation des secrets** : mot de passe DSRM (Directory Services Restore Mode), clés de récupération BitLocker, mots de passe des comptes de service, stockés dans un coffre-fort physique -- jamais uniquement dans un gestionnaire de mots de passe connecté au réseau.

Erreur fréquente : la sauvegarde AD dans le périmètre réseau
Nous observons régulièrement que les sauvegardes AD sont stockées sur des partages réseau accessibles depuis le domaine. Un attaquant ayant compromis un compte Domain Admin peut détruire ces sauvegardes. La sauvegarde AD critique doit être physiquement déconnectée ou stockée dans un vault immuable avec authentification hors-domaine.

6. Reconstruction Active Directory : procédure de référence

6.1 Les deux approches de reconstruction

Après une compromission confirmée de l'AD, deux approches sont possibles :

Approche 1 : Restauration d'une sauvegarde saine. Si l'on dispose d'une sauvegarde System State antérieure à la compromission (identifiée grâce à la timeline forensique), il est possible de restaurer les contrôleurs de domaine à un état sain. Cette approche est plus rapide mais comporte un risque : si la date de compromission initiale est mal estimée, les backdoors seront restaurées avec la sauvegarde.

Approche 2 : Reconstruction from scratch (forêt vierge). C'est l'approche la plus sûre mais aussi la plus longue. Elle consiste à créer une nouvelle forêt AD, migrer les objets nécessaires depuis un export de l'ancienne forêt (après nettoyage), et redéployer progressivement les services. Cette approche est recommandée en cas de compromission profonde (Golden Ticket, persistence au niveau des certificats ADCS).

6.2 Étapes de reconstruction from scratch

1. **Environnement isolé :** Installer un environnement réseau physiquement isolé (air-gapped) pour la reconstruction. Aucune connexion avec le réseau compromis.
2. **Premier DC :** Installer un serveur propre (OS fraîchement installé, non joint au domaine compromis), promouvoir en contrôleur de domaine d'une nouvelle forêt avec un nouveau nom de domaine.
3. **Durcissement immédiat :** Appliquer l'ensemble des mesures de durcissement AD dès la création : politique de mots de passe forte, Tiering administratif, LAPS, désactivation des protocoles obsolètes (NTLMv1, LM hash).
4. **Import des objets :** Importer les utilisateurs, groupes et OU depuis un export nettoyé. Ne pas importer les comptes de service sans vérification individuelle. Forcer le changement de mot de passe pour tous les utilisateurs.
5. **PKI :** Déployer une nouvelle infrastructure de certificats (PKI/ADCS) avec de nouvelles autorités de certification. Ne jamais réutiliser les clés CA de l'ancienne infrastructure.
6. **Tests :** Valider l'intégrité de l'annuaire, la réplication entre DC, le fonctionnement DNS et les stratégies de groupe avant toute mise en production.
7. **Migration progressive :** Migrer les postes de travail et serveurs vers la nouvelle forêt par lots, en commençant par les systèmes les plus critiques.

7. Cellule de crise et communication

7.1 Composition et activation de la cellule de crise

La cellule de crise cyber doit être prédéfinie, documentée et exercée régulièrement. Sa composition type inclut :

- **Directeur de crise** : membre du COMEX, autorité décisionnelle (DG, DAF ou DSI selon la gouvernance)
- **RSSI** : pilotage technique de la réponse, interface avec les prestataires cyber
- **DSI** : coordination des équipes IT pour la reconstruction
- **Responsable juridique** : notifications réglementaires (CNIL, ANSSI), gestion contractuelle

- **Responsable communication** : communication interne, externe, média, réseaux sociaux
- **DRH** : gestion du personnel, communication aux salariés, recours à des renforts
- **Responsable métier** : priorisation des processus métier à restaurer
- **Prestataire forensique** : investigation technique, identification du vecteur d'attaque

Point critique : moyens de communication alternatifs
Si le SI est intégralement chiffré, les moyens de communication habituels (messagerie, Teams, téléphonie IP) sont indisponibles. La cellule de crise doit disposer de **moyens de communication hors SI** : téléphones mobiles personnels avec annuaire papier, messagerie Signal ou WhatsApp sur mobiles personnels, salle de réunion physique prédéfinie. Ces éléments doivent être documentés dans une fiche réflexe accessible sans connexion au SI (format papier ou clé USB).

7.2 Communication de crise : les règles essentielles

La communication pendant une crise cyber obéit à des règles strictes :

- **Communication interne en premier :** les collaborateurs doivent être informés avant les médias. Un message clair et factuel, sans minimiser ni dramatiser.
- **Porte-parole unique :** toute communication externe passe par un interlocuteur unique, formé à la communication de crise.
- **Ne jamais révéler les détails techniques :** ne pas communiquer sur le vecteur d'attaque, les systèmes affectés ou les négociations avec les attaquants.
- **Notifications réglementaires dans les délais :** CNIL sous 72h en cas de violation de données personnelles, ANSSI pour les OIV et entités NIS 2, autorités sectorielles le cas échéant.
- **Anticiper les questions :** préparer des Q&A pour les clients, partenaires, actionnaires et médias.

8. Exercices de simulation et RETEX

8.1 Types d'exercices

Un PRA/PCA non testé est un PRA/PCA qui échouera le jour J. Les exercices doivent être réguliers, progressifs et couvrir différents niveaux de complexité :

Type d'exercice	Fréquence recommandée	Objectif	Participants
Revue documentaire	Semestrielle	Vérifier l'actualité et la cohérence des plans	RSSI, DSI
Exercice sur table (tabletop)	Annuelle	Tester les processus décisionnels face à un scénario	Cellule de crise complète
Test technique partiel	Trimestrielle	Valider la restauration d'un système critique	Equipes IT / Backup
Exercice grandeur nature	Annuelle	Simulation complète incluant communication de crise	Toute l'organisation
Test de restauration AD	Semestrielle	Restaurer un DC dans un environnement isolé	Equipe AD / Sécurité

8.2 Méthodologie d'exercice tabletop

L'exercice tabletop est le format le plus accessible et le plus riche en enseignements. Voici une méthodologie éprouvée :

1. **Préparation (2 semaines avant) :** définir le scénario, préparer les injects (messages simulant l'évolution de la crise), convoquer les participants, réserver la salle.
2. **Introduction (15 min) :** rappeler les règles du jeu, présenter le contexte de départ ("Il est 6h lundi matin, le SOC vous appelle...").
3. **Injection séquentielle (2-3h) :** soumettre les injects toutes les 15-20 minutes, forçant les participants à prendre des décisions sous pression et avec des informations incomplètes.
4. **Débriefing à chaud (30 min) :** recueillir les impressions des participants, identifier les points de blocage immédiats.
5. **RETEX formel (1 semaine après) :** rédiger un rapport structuré avec les constats (positifs et négatifs), les actions correctives et les responsables associés.

8.3 RETEX : transformer l'expérience en amélioration

Le **Retour d'Expérience (RETEX)** est la clé de l'amélioration continue. Qu'il soit issu d'un exercice ou d'un incident réel, le RETEX doit suivre une structure formelle :

- **Chronologie factuelle :** reconstitution minute par minute des événements et décisions
- **Ce qui a fonctionné :** identifier et valoriser les bonnes pratiques
- **Ce qui a échoué :** identifier les défaillances sans chercher de coupables (culture "blame-free")
- **Actions correctives :** chaque constat négatif doit générer une action avec un responsable et une échéance
- **Suivi :** les actions correctives doivent être suivies dans un registre et vérifiées lors de l'exercice suivant

Un exercice de type Purple Team peut compléter utilement les exercices de crise en testant les capacités de détection et de réponse technique face à des scénarios d'attaque réalistes.

9. Intégration réglementaire : NIS 2, DORA, ISO 22301

9.1 Exigences NIS 2 en matière de continuité

La directive NIS 2 (article 21) impose aux entités essentielles et importantes des mesures de gestion des risques incluant explicitement :

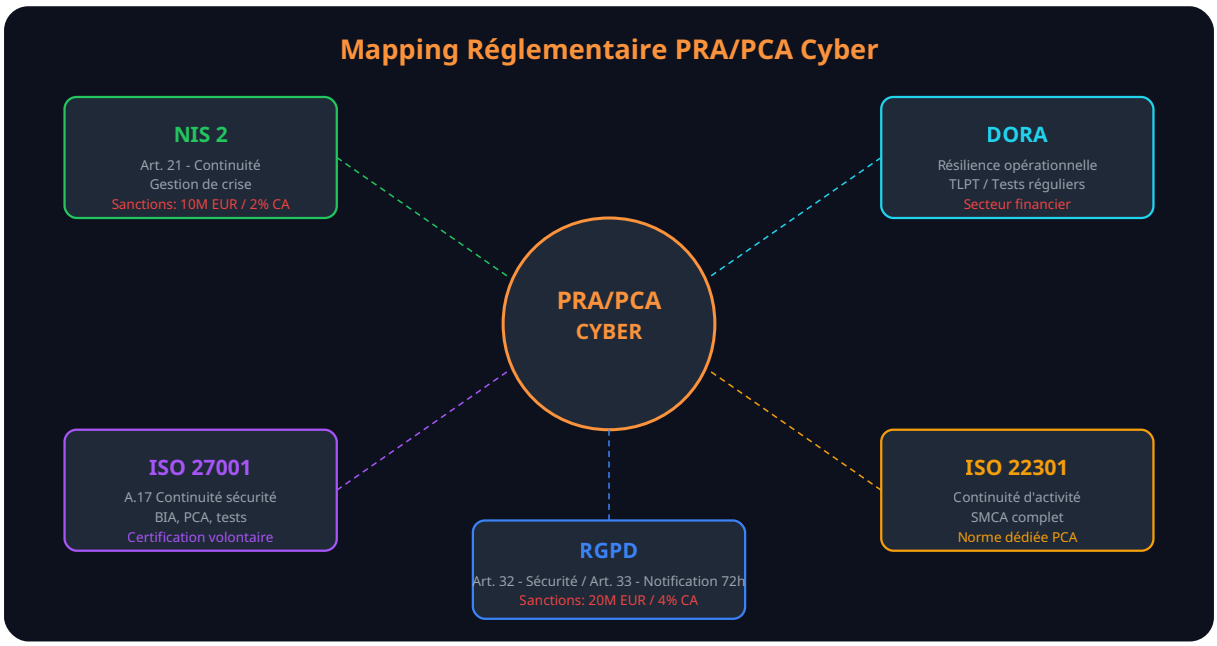
- La **continuité des activités**, y compris la gestion des sauvegardes et la reprise après sinistre
- La **gestion des crises**, incluant les procédures d'escalade et de communication
- La **sécurité de la chaîne d'approvisionnement**, avec évaluation des fournisseurs
- Des **tests réguliers** d'efficacité des mesures de gestion des risques

Les sanctions pour non-conformité peuvent atteindre **10 millions d'euros ou 2 % du CA mondial** pour les entités essentielles. La directive prévoit également la responsabilité personnelle des dirigeants, qui doivent approuver les mesures de gestion des risques et suivre une formation en cybersécurité.

9.2 Exigences DORA pour le secteur financier

Le règlement DORA, applicable depuis janvier 2025, va plus loin que NIS 2 pour le secteur financier :

- **Tests de résilience opérationnelle numérique** obligatoires, incluant des scénarios d'attaque cyber
- **Threat-Led Penetration Testing (TLPT)** pour les entités significatives, basé sur le framework TIBER-EU
- **Gestion des risques liés aux tiers prestataires TIC**, incluant des plans de sortie et de continuité
- **Notification des incidents majeurs** aux autorités de surveillance financière



9.3 ISO 22301 : le référentiel de la continuité d'activité

La norme **ISO 22301** est le standard international dédié au management de la continuité d'activité. Elle fournit un cadre complet pour établir, implémenter, maintenir et améliorer un SMCA (Système de Management de la Continuité d'Activité). Bien que non spécifique au cyber, elle constitue le socle méthodologique idéal pour structurer un PRA/PCA Cyber, en complément de l'ISO 27001 pour les aspects sécurité de l'information.

Pour approfondir ce sujet, consultez notre outil open-source pci-dss-audit-tool qui facilite l'audit de conformité PCI DSS.

10. Checklist PRA/PCA Cyber : les 30 points essentiels

Utilisez cette checklist pour évaluer la maturité de votre PRA/PCA Cyber. Chaque point non validé représente une vulnérabilité potentielle de votre capacité de résilience :

Gouvernance et Organisation

- Le PRA/PCA Cyber est un document distinct du PRA classique
- Un BIA a été réalisé avec implication des métiers dans les 12 derniers mois
- Les RTO/RPO sont définis pour chaque processus critique et validés par la Direction
- La cellule de crise est constituée, avec des remplaçants désignés
- Un annuaire de crise papier (ou hors SI) est maintenu à jour
- Des moyens de communication hors SI sont identifiés et testés

Sauvegardes

- La stratégie 3-2-1-1-0 est appliquée pour les données critiques
- Une copie de sauvegarde est physiquement offline ou immuable
- Les sauvegardes AD (System State + bare metal) sont effectuées quotidiennement
- Le mot de passe DSRM est documenté et accessible hors SI

- Les tests de restauration sont effectués mensuellement
- Les durées de rétention sont cohérentes avec les RPO définis

Procédures de reprise

- Une procédure de reconstruction AD from scratch est documentée et testée
- L'ordre de redémarrage des systèmes est défini et documenté
- Les procédures de vérification d'intégrité post-restauration existent
- Un environnement de reconstruction isolé est disponible (ou rapidement déployable)
- Les configurations de référence (golden images, IaC) sont stockées hors du périmètre compromis

Communication et juridique

- Des modèles de communication de crise sont prêts (interne, clients, médias)
- Le processus de notification CNIL sous 72h est formalisé
- Un contrat de réponse à incident est en place avec un prestataire qualifié
- La couverture cyber-assurance est adéquate et les conditions de déclenchement sont connues
- Les obligations contractuelles envers les clients sont identifiées

Exercices et amélioration continue

- Un exercice tabletop est réalisé annuellement
- Un test technique de restauration complète est réalisé annuellement
- Les RETEX sont formalisés avec des actions correctives suivies
- Le PRA/PCA est mis à jour après chaque exercice et changement majeur du SI
- Les scénarios d'exercice sont variés (ransomware, compromission AD, supply chain, exfiltration)
- La conformité NIS 2 / DORA est vérifiée dans le PRA/PCA

Sources et références : CNIL · ANSSI

Questions frequentes

Comment mettre en place PRA/PCA Cyber dans un environnement de production ?

La mise en place de PRA/PCA Cyber en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi PRA/PCA Cyber est-il essentiel pour la securite des systemes d'information ?

PRA/PCA Cyber constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quel est le délai réaliste pour se mettre en conformité avec PRA/PCA Cyber : Plan de Reprise et Continuité d'Activité ?

Comptez entre 6 et 18 mois selon la maturité de votre SI. Les entreprises qui partent de zéro doivent prévoir 12 mois minimum avec un accompagnement externe dédié.

> Points clés à retenir
>
> - 4. Scénarios cyber majeurs à intégrer dans le PRA
> - 5. Stratégie de sauvegarde 3-2-1-1-0 : le bouclier ultime
> - 6. Reconstruction Active Directory : procédure de référence
> - 7. Cellule de crise et communication
> - 8. Exercices de simulation et RETEX
> - 9. Intégration réglementaire : NIS 2, DORA, ISO 22301

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr