

Checklist de préparation à la cybercrise

Checklist de préparation à la cybercrise

Introduction

Les cyberattaques sont devenues l'une des menaces les plus probables et les plus coûteuses pour les organisations de toutes tailles. Cette checklist complète vous aidera à évaluer votre niveau de préparation face à une cyberattaque ou une violation de données, et à identifier les points d'amélioration pour renforcer votre résilience.

Dans un contexte où la surface d'attaque des organisations ne cesse de s'étendre (télétravail, cloud, objets connectés, chaîne d'approvisionnement...), la question n'est plus de savoir si votre organisation sera ciblée, mais quand et comment vous y répondrez. Les coûts moyens d'une cyberattaque ont dépassé les 4,5 millions d'euros en 2024, avec des impacts qui vont bien au-delà des aspects purement techniques : perte de données, interruption d'activité, atteinte à la réputation, sanctions réglementaires, et dans les cas les plus graves, menace sur la pérennité même de l'organisation.

Cette checklist couvre les aspects essentiels d'une préparation complète à la cybercrise, regroupés en sept domaines clés. Elle a été conçue pour être applicable à des organisations de toutes tailles et de tous secteurs, tout en mettant en évidence les mesures prioritaires.

Comment utiliser cette checklist

Pour chaque élément, cochez “Oui” si la mesure est en place et complètement opérationnelle, “Partiel” si elle est en cours de développement ou incomplète, et “Non” si elle n’est pas encore mise en œuvre. Les éléments marqués d’un astérisque (*) sont considérés comme prioritaires.

Nous vous recommandons de :

1. Réaliser une première évaluation complète pour établir votre niveau initial
2. Identifier les écarts les plus critiques (mesures prioritaires non implémentées)
3. Élaborer un plan d’action avec des échéances réalistes
4. Réévaluer régulièrement (tous les 6 mois) pour mesurer les progrès

Cette checklist peut être utilisée par différents acteurs au sein de votre organisation :

- Direction des systèmes d’information (DSI)
- Responsable de la sécurité des systèmes d’information (RSSI)
- Direction générale
- Responsables de la continuité d’activité
- Auditeurs internes

1. Gouvernance et organisation

Une bonne gouvernance constitue le fondement d’un dispositif de cybersécurité efficace. Elle garantit que les enjeux de sécurité sont pris en compte au plus haut niveau de l’organisation et que les responsabilités sont clairement définies.

Mesure	Oui	Partiel	Non
<i>Une politique de sécurité des systèmes d’information est formalisée et approuvée par la direction</i>	☐	☐	☐
Un responsable de la sécurité des systèmes d’information (RSSI) est désigné	☐	☐	☐
Les rôles et responsabilités en matière de cybersécurité sont clairement définis	☐	☐	☐

Mesure	Oui	Partiel	Non
<i>Un plan de réponse aux incidents cyber est formalisé et régulièrement mis à jour</i>	☐	☐	☐
Une cellule de crise cyber est constituée et formée	☐	☐	☐
Des exercices de simulation de cybercrise sont régulièrement organisés	☐	☐	☐
Des indicateurs de performance en matière de cybersécurité sont suivis par la direction	☐	☐	☐

Bonnes pratiques et conseils

Politique de sécurité des systèmes d'information (PSSI)

La PSSI doit être :

- Adaptée aux spécificités et aux risques de votre organisation
- Formalisée dans un document clair et accessible
- Approuvée formellement par la direction générale
- Communiquée à l'ensemble des collaborateurs
- Révisée au moins une fois par an

Un document PSSI efficace contient généralement :

- Les objectifs de sécurité de l'organisation
- Le cadre réglementaire applicable
- Les principes directeurs de sécurité
- Les responsabilités des différents acteurs
- Les références aux procédures détaillées

Désignation d'un RSSI

Selon la taille de votre organisation, le RSSI peut être :

- Un poste à temps plein dans les grandes organisations
- Une fonction partiellement déléguée à un collaborateur existant dans les PME
- Une prestation externalisée (RSSI virtuel) pour les plus petites structures

L'essentiel est que cette personne :

- Dispose des compétences techniques et organisationnelles nécessaires
- Soit positionnée à un niveau hiérarchique adéquat
- Bénéficie d'un accès direct à la direction générale
- Dispose de l'indépendance nécessaire vis-à-vis de la DSI

Plan de réponse aux incidents

Un plan de réponse efficace doit :

- Définir les critères de qualification et de priorisation des incidents
- Établir une procédure claire d'escalade et de notification
- Identifier les ressources internes et externes mobilisables
- Prévoir des procédures de collecte de preuves (forensics)
- Inclure des templates de communication interne et externe
- Être testé régulièrement via des exercices de simulation

Exercices de simulation

Des exercices réguliers permettent de :

- Tester l'efficacité des procédures en conditions réelles
- Former les équipes à réagir sous pression
- Identifier les points faibles du dispositif
- Renforcer la collaboration entre les différentes fonctions
- Démontrer l'engagement de la direction

Types d'exercices à envisager :

- Exercices sur table (tabletop) : simulation théorique avec les décideurs
- Tests techniques : vérification des capacités de détection et réponse
- Simulation complète (red team) : test de pénétration non annoncé
- Exercice inter-organisations : coordination avec partenaires et autorités

2. Protection des données et des systèmes

La protection constitue la première ligne de défense contre les cyberattaques. Elle vise à réduire la surface d'exposition et à renforcer la résistance de vos

systèmes face aux tentatives d'intrusion.

Mesure	Oui	Partiel	Non
<i>Un inventaire des actifs informatiques et des données sensibles est maintenu à jour</i>	☐	☐	☐
<i>Une politique de sauvegarde régulière est mise en œuvre avec tests de restauration</i>	☐	☐	☐
<i>Un système de protection contre les malwares est déployé et maintenu à jour</i>	☐	☐	☐
Une segmentation du réseau est mise en place	☐	☐	☐
<i>Les mises à jour de sécurité sont déployées régulièrement sur tous les systèmes</i>	☐	☐	☐
Un système de gestion des accès est en place avec authentification forte	☐	☐	☐
Le principe du moindre privilège est appliqué pour les droits d'accès	☐	☐	☐
<i>Le chiffrement des données sensibles est mis en œuvre</i>	☐	☐	☐
Des solutions de protection des terminaux (EDR) sont déployées	☐	☐	☐

Bonnes pratiques et conseils

Inventaire des actifs et données

Un inventaire efficace doit :

- Répertorier tous les équipements connectés au réseau
- Identifier les systèmes critiques pour l'activité
- Classifier les données selon leur sensibilité
- Documenter les interdépendances entre systèmes
- Être mis à jour après chaque changement significatif

Outils recommandés :

- Solutions de découverte automatique du réseau
- Logiciels de gestion des actifs informatiques (ITAM)
- Registre des traitements de données personnelles
- Cartographie des flux de données

Politique de sauvegarde

Une stratégie de sauvegarde robuste doit suivre le principe 3-2-1 :

- 3 copies des données au minimum
- 2 supports de stockage différents
- 1 copie stockée hors site (ou dans le cloud)

Points essentiels :

- Définir la fréquence des sauvegardes selon la criticité
- Automatiser le processus autant que possible
- Chiffrer les sauvegardes contenant des données sensibles
- Tester régulièrement la restauration (au moins trimestriellement)
- Prévoir des sauvegardes hors ligne (air gap) pour se prémunir des ransomwares

Protection contre les malwares

Une protection efficace combine plusieurs niveaux :

- Antivirus/antimalware sur tous les postes et serveurs
- Protection des messageries (filtrage des pièces jointes, anti-spam)
- Sécurisation de la navigation web (filtrage URL, proxy sécurisé)
- Solution EDR (Endpoint Detection and Response) pour une détection avancée
- Sensibilisation des utilisateurs aux risques

Les solutions doivent être :

- Mises à jour automatiquement (signatures et moteurs)
- Centralisées pour une gestion et une supervision efficaces
- Configurées pour remonter des alertes en temps réel
- Régulièrement auditées pour vérifier leur couverture

Segmentation du réseau

La segmentation permet de limiter la propagation latérale d'une attaque en :

- Isolant les systèmes critiques dans des zones protégées
- Séparant les réseaux de production, de test et d'administration
- Contrôlant les flux entre les différentes zones
- Protégeant spécifiquement les systèmes industriels (OT)
- Isolant les équipements IoT du réseau principal

Technologies à considérer :

- VLANs et pare-feux internes
- Micro-segmentation (Zero Trust Network)
- Passerelles sécurisées entre zones
- NAC (Network Access Control)

Gestion des accès et authentification

Une gestion des accès robuste repose sur :

- L'authentification multifacteur (MFA) pour tous les accès sensibles
- Une politique de mots de passe forte et adaptée
- La gestion centralisée des identités (IAM)
- Des procédures rigoureuses de création/suppression de comptes
- Des revues périodiques des droits d'accès

Le principe du moindre privilège implique :

- D'attribuer uniquement les droits nécessaires à la fonction
- De limiter le nombre de comptes à privilèges étendus
- D'utiliser des comptes distincts pour les fonctions administratives
- De réévaluer régulièrement les besoins d'accès

3. Détection et surveillance

La détection rapide d'une intrusion ou d'une activité suspecte est cruciale pour limiter l'impact d'une cyberattaque. Un temps de détection moyen inférieur à 24 heures peut réduire significativement le coût d'un incident.

Mesure	Oui	Partiel	Non
<i>Un système de détection d'intrusion est en place</i>	☐	☐	☐
Une surveillance 24/7 des systèmes critiques est assurée	☐	☐	☐
Des journaux d'événements sont collectés et analysés régulièrement	☐	☐	☐
<i>Des alertes automatiques sont configurées pour les comportements suspects</i>	☐	☐	☐
Un processus d'escalade des incidents de sécurité est défini	☐	☐	☐
Des tests d'intrusion sont réalisés périodiquement	☐	☐	☐
Une veille sur les vulnérabilités est organisée	☐	☐	☐

Bonnes pratiques et conseils

Systèmes de détection

Un dispositif de détection complet comprend :

- Des IDS/IPS (Intrusion Detection/Prevention System) réseau
- Des solutions EDR sur les postes et serveurs
- Des sondes applicatives pour les applications critiques
- Des outils de détection des anomalies comportementales
- Des systèmes de détection des fuites de données (DLP)

Points d'attention :

- Calibrer les systèmes pour limiter les faux positifs
- Maintenir les signatures et règles à jour
- Assurer une couverture de tous les points d'entrée potentiels
- Prévoir la détection des techniques d'attaque avancées (APT)

Collecte et analyse des journaux

Une gestion efficace des logs nécessite :

- La centralisation des journaux de tous les systèmes critiques
- La synchronisation des horloges pour une analyse chronologique
- Une politique de rétention adaptée aux besoins réglementaires
- Des outils d'analyse automatisée (SIEM)
- Des procédures de sauvegarde et protection des logs

Événements à surveiller en priorité :

- Connexions administratives et privilégiées
- Activités en dehors des heures habituelles
- Volumes inhabituels de transfert de données
- Modifications des configurations de sécurité
- Échecs d'authentification répétés

Surveillance 24/7

Selon vos ressources, différentes options sont possibles :

- Équipe interne de sécurité opérationnelle (SOC)
- Service externalisé de surveillance (MSSP)
- Solution hybride avec outils automatisés et astreinte
- Solution mutualisée pour les petites structures

L'essentiel est de garantir :

- Une capacité de détection en continu
- Un temps de réaction adapté à vos enjeux
- Des procédures claires pour les analystes
- Une chaîne d'escalade bien définie

Tests d'intrusion

Les tests d'intrusion doivent être :

- Réalisés par des équipes qualifiées (internes ou externes)
- Conduits selon une méthodologie reconnue (OSSTMM, PTES...)
- Adaptés aux risques spécifiques de votre organisation
- Suivis d'un plan de remédiation des vulnérabilités identifiées
- Répétés après des changements significatifs d'infrastructure

Fréquence recommandée :

- Systèmes critiques exposés : tous les 6 mois
- Applications web exposées : après chaque changement majeur
- Infrastructure interne : annuellement

Veille sur les vulnérabilités

Un processus de veille efficace comprend :

- Le suivi des alertes des fournisseurs de vos solutions
- L'abonnement aux bulletins de sécurité nationaux (CERT, ANSSI...)
- La surveillance des bases de vulnérabilités (CVE, NVD)
- L'utilisation d'outils de scan de vulnérabilités
- L'évaluation rapide de l'applicabilité à votre contexte

La veille doit être suivie d'un processus de gestion des vulnérabilités avec :

- Évaluation de la criticité
- Priorisation selon le risque
- Planification des correctifs
- Validation de l'efficacité des corrections

4. Réponse aux incidents

Même avec les meilleures protections, un incident peut survenir. Une capacité de réponse efficace permet de contenir rapidement la menace, de limiter les dommages et de restaurer les opérations normales.

Mesure	Oui	Partiel	Non
<i>Une procédure de gestion des incidents cyber est formalisée</i>	☐	☐	☐
<i>Les contacts d'urgence internes et externes sont tenus à jour</i>	☐	☐	☐
Des ressources techniques sont disponibles pour l'investigation	☐	☐	☐

Mesure	Oui	Partiel	Non
Une procédure d'isolement des systèmes compromis est définie	☐	☐	☐
<i>Un plan de communication de crise cyber est préparé</i>	☐	☐	☐
Les obligations légales de notification sont identifiées	☐	☐	☐
Un contrat avec un prestataire spécialisé en réponse à incident est en place	☐	☐	☐

Bonnes pratiques et conseils

Procédure de gestion des incidents

Une procédure efficace suit généralement les phases du NIST (National Institute of Standards and Technology) :

1. **Préparation** : ressources, outils et formation
2. **Détection et analyse** : identification et évaluation de l'incident
3. **Confinement** : limitation de la propagation
4. **Éradication** : suppression de la menace
5. **Récupération** : restauration des systèmes
6. **Capitalisation** : documentation et leçons apprises

Pour chaque phase, la procédure doit préciser :

- Les actions à réaliser
- Les responsables de chaque action
- Les outils et ressources nécessaires
- Les critères de passage à la phase suivante

Contacts d'urgence

Maintenez un annuaire à jour comprenant :

Contacts internes :

- Membres de la cellule de crise
- Experts techniques par domaine

- Responsables métiers
- Direction générale
- Service juridique
- Communication

Contacts externes :

- Autorités compétentes (ANSSI, CNIL, forces de l'ordre)
- Prestataires spécialisés en réponse à incident
- Assistance des éditeurs et fournisseurs critiques
- Assureur cyber (si applicable)
- Conseil juridique spécialisé

L'annuaire doit être :

- Accessible même en cas de compromission du système d'information
- Disponible en version papier et numérique sécurisée
- Testé régulièrement pour vérifier la validité des contacts
- Mis à jour après chaque changement organisationnel

Ressources d'investigation

Les ressources minimales comprennent :

- Outils d'analyse forensique (capture de mémoire, analyse de disque)
- Logiciels d'analyse de logs et de trafic réseau
- Environnement isolé pour l'analyse des malwares
- Documentation technique des systèmes
- Moyens de communication sécurisés (non compromis)

Ces ressources peuvent être :

- Internalisées avec des équipes formées
- Externalisées auprès de prestataires spécialisés
- Hybrides avec une capacité de première intervention interne

Plan de communication de crise cyber

Un plan de communication efficace prévoit :

- Des modèles préparés pour différents scénarios
- Une stratégie de communication adaptée à chaque partie prenante
- Des points réguliers sur l'avancement de la résolution
- Des porte-parole désignés et formés
- Une coordination avec les autorités concernées

Parties prenantes à considérer :

- Collaborateurs
- Clients et partenaires
- Autorités de régulation
- Médias
- Grand public (selon l'impact)

Obligations légales de notification

Identifiez à l'avance vos obligations en matière de :

- Notification des violations de données personnelles (RGPD : 72h)
- Déclaration aux autorités sectorielles (finance, santé, énergie...)
- Information des personnes concernées par une fuite de données
- Signalement aux services de cybersécurité nationaux
- Déclaration aux autorités judiciaires en cas d'infraction

Préparez des modèles de notification conformes aux exigences légales et incluant :

- La nature de l'incident
- Les catégories et le volume de données concernées
- Les conséquences probables
- Les mesures prises ou envisagées

5. Continuité et reprise d'activité

La capacité à maintenir les fonctions essentielles pendant une crise et à restaurer rapidement les opérations normales est cruciale pour limiter l'impact financier et réputationnel d'une cyberattaque.

Mesure	Oui	Partiel	Non
<i>Un plan de continuité d'activité incluant les scénarios cyber est formalisé</i>	☐	☐	☐
Des procédures de fonctionnement en mode dégradé sont définies	☐	☐	☐
<i>Une stratégie de sauvegarde et restauration est documentée et testée</i>	☐	☐	☐
Des sauvegardes hors ligne (air gap) sont mises en place	☐	☐	☐
Les délais de reprise d'activité sont définis pour chaque système critique	☐	☐	☐
Des tests de reprise après sinistre sont effectués régulièrement	☐	☐	☐
Des sites de repli sont identifiés et opérationnels	☐	☐	☐

Bonnes pratiques et conseils

Plan de continuité d'activité (PCA)

Un PCA efficace face aux cybermenaces doit :

- Identifier les processus métiers critiques
- Définir les ressources minimales nécessaires
- Prévoir des procédures manuelles de substitution
- Établir une organisation de crise claire
- Couvrir différents scénarios (ransomware, DDoS, fuite de données...)

Éléments spécifiques aux cybercrises :

- Procédures d'isolation réseau d'urgence
- Moyens de communication alternatifs (non dépendants du SI)
- Accès aux ressources critiques en cas de compromission des systèmes d'authentification
- Priorisation des systèmes à restaurer

Fonctionnement en mode dégradé

Pour chaque activité critique, définissez :

- Le niveau de service minimal acceptable
- Les moyens alternatifs (manuels, solutions de contournement)
- Les ressources nécessaires (humaines et matérielles)
- Les procédures exceptionnelles (simplification des processus)
- Les critères de retour au mode normal

Exemples de mesures :

- Formulaires papier pré-imprimés pour remplacer les applications critiques
- Procédures manuelles de traitement des opérations essentielles
- Équipes renforcées pour compenser l'absence d'automatisation
- Communication directe en cas d'indisponibilité des systèmes de messagerie

Stratégie de sauvegarde et restauration

Une stratégie complète intègre :

- **RPO** (Recovery Point Objective) : perte de données maximale acceptable
- **RTO** (Recovery Time Objective) : temps maximal de restauration
- Priorisation des systèmes et données à restaurer
- Procédures détaillées de restauration
- Ressources nécessaires (matériel, logiciel, personnel)

Spécificités liées aux cybermenaces :

- Protection contre les ransomwares (sauvegardes hors ligne)
- Validation de l'intégrité des sauvegardes
- Procédures de restauration en environnement potentiellement compromis
- Tests réguliers de restauration complète

Tests de reprise

Les tests doivent être :

- Variés dans leur périmètre et leur ambition

- Planifiés régulièrement (au moins annuellement)
- Documentés et évalués formellement
- Suivis de plans d'amélioration

Types de tests à envisager :

- Tests théoriques (revue documentaire)
- Tests techniques isolés (restauration de composants spécifiques)
- Tests partiels (restauration d'environnements non-productifs)
- Exercices complets (simulation d'un sinistre majeur)

Sites de repli

Selon vos besoins, différentes options sont possibles :

- Site de secours chaud (immédiatement opérationnel)
- Site de secours tiède (opérationnel sous quelques heures)
- Site de secours froid (opérationnel sous quelques jours)
- Solutions cloud de disaster recovery (DRaaS)
- Accords de réciprocité avec d'autres organisations

Critères de sélection :

- Séparation géographique du site principal
- Capacité à héberger les équipes essentielles
- Infrastructures techniques adaptées
- Connectivité réseau appropriée
- Sécurité physique et logique

6. Formation et sensibilisation

L'humain reste le maillon essentiel de la cybersécurité. Un programme efficace de formation et de sensibilisation réduit considérablement le risque d'incidents et améliore la réponse collective en cas de crise.

Mesure	Oui	Partiel	Non
<i>Un programme de sensibilisation à la cybersécurité est déployé pour tous les collaborateurs</i>	☐	☐	☐

Mesure	Oui	Partiel	Non
<i>Des formations spécifiques sont dispensées aux équipes IT</i>	☐	☐	☐
Des campagnes de phishing simulé sont régulièrement organisées	☐	☐	☐
Les nouveaux collaborateurs reçoivent une formation sur la sécurité	☐	☐	☐
La direction est sensibilisée aux enjeux et risques cyber	☐	☐	☐
Des rappels réguliers sur les bonnes pratiques sont diffusés	☐	☐	☐
Un canal pour signaler les incidents est connu de tous	☐	☐	☐

Bonnes pratiques et conseils

Programme de sensibilisation

Un programme efficace doit être :

- Adapté aux différents profils de collaborateurs
- Régulier et non limité à une session annuelle
- Concret avec des exemples réels et contextualisés
- Engageant et non culpabilisant
- Évalué pour mesurer son impact

Thématiques essentielles à couvrir :

- Reconnaissance des tentatives de phishing
- Gestion des mots de passe et authentification
- Sécurité en mobilité et télétravail
- Protection des données sensibles
- Utilisation des médias sociaux
- Procédures de signalement des incidents

Formations spécifiques IT

Les équipes techniques doivent recevoir des formations sur :

- Développement sécurisé (pour les développeurs)
- Configuration sécurisée des systèmes
- Gestion des vulnérabilités
- Détection et réponse aux incidents
- Architecture de sécurité
- Conformité réglementaire

Options de formation :

- Certifications reconnues (CISSP, CEH, OSCP...)
- Formations sur mesure adaptées à votre environnement
- Plateformes d'entraînement (CTF, labs virtuels)
- Conférences et communautés professionnelles

Campagnes de phishing simulé

Pour être efficaces, ces campagnes doivent :

- Être progressives dans leur sophistication
- Reproduire des scénarios d'attaque réalistes et actuels
- Être suivies de sensibilisation immédiate en cas d'échec
- Mesurer l'évolution des taux de clics sur la durée
- Éviter la stigmatisation des collaborateurs qui échouent

Bonnes pratiques :

- Commencer par des scénarios simples
- Organiser au moins une campagne par trimestre
- Varier les thèmes et approches
- Renforcer la formation pour les groupes à risque
- Communiquer sur les résultats globaux

Sensibilisation de la direction

La direction doit être spécifiquement sensibilisée sur :

- Les risques cyber majeurs pour l'organisation
- Les responsabilités légales et réglementaires

- Les impacts financiers potentiels
- Les décisions stratégiques en matière de cybersécurité
- Son rôle exemplaire en matière de bonnes pratiques

Formats adaptés :

- Sessions dédiées et synthétiques
- Benchmarks sectoriels
- Retours d'expérience d'incidents réels
- Exercices de simulation de crise
- Reporting régulier sur les indicateurs clés

Canaux de signalement

Les collaborateurs doivent connaître :

- Comment reconnaître un incident de sécurité potentiel
- À qui et comment le signaler rapidement
- Les informations à fournir
- Les actions immédiates à prendre ou à éviter
- L'importance d'un signalement rapide même en cas de doute

Le dispositif doit garantir :

- Simplicité d'utilisation
- Accessibilité 24/7
- Absence de sanction pour les signalements de bonne foi
- Suivi et retour sur les signalements
- Confidentialité appropriée

7. Gestion des tiers et de la chaîne d'approvisionnement

La chaîne d'approvisionnement est devenue un vecteur d'attaque majeur. Une gestion rigoureuse des risques liés aux tiers est essentielle pour protéger votre organisation des menaces indirectes.

Mesure	Oui	Partiel	Non
<i>Les exigences de sécurité sont incluses dans les contrats avec les fournisseurs</i>	☐	☐	☐
Une évaluation de la sécurité des fournisseurs critiques est réalisée	☐	☐	☐
Les accès des prestataires externes sont strictement contrôlés	☐	☐	☐
Des clauses de notification d'incident sont prévues dans les contrats	☐	☐	☐
Une cartographie des interconnexions avec les tiers est maintenue	☐	☐	☐
Les responsabilités en cas d'incident sont clairement définies	☐	☐	☐

Bonnes pratiques et conseils

Exigences contractuelles

Les contrats avec les fournisseurs critiques doivent inclure :

- Des engagements de niveau de sécurité (référentiels, certifications)
- Des clauses d'audit et de contrôle
- Des obligations de notification en cas d'incident
- Des garanties sur la protection des données
- Des pénalités en cas de manquement
- Des conditions de réversibilité

Adaptez le niveau d'exigence selon :

- La criticité du service pour votre activité
- La sensibilité des données accessibles
- Le niveau d'interconnexion avec vos systèmes
- Les obligations réglementaires applicables

Évaluation des fournisseurs

L'évaluation doit être :

- Proportionnée aux risques identifiés
- Basée sur des critères objectifs et mesurables
- Réalisée avant la contractualisation puis périodiquement
- Documentée et suivie dans le temps

Méthodes d'évaluation :

- Questionnaires d'auto-évaluation
- Revue documentaire (politiques, certifications)
- Audits sur site ou à distance
- Tests techniques (scan de vulnérabilités, pentest)
- Évaluation par un tiers indépendant

Contrôle des accès prestataires

Les accès accordés aux tiers doivent être :

- Limités au strict nécessaire (moindre privilège)
- Temporaires et révisés régulièrement
- Surveillés et journalisés
- Protégés par une authentification forte
- Activés via des canaux sécurisés (VPN, bastion)

Bonnes pratiques :

- Créer des comptes nominatifs (éviter les comptes partagés)
- Mettre en place des solutions de gestion des accès privilégiés (PAM)
- Prévoir des procédures de révocation rapide
- Revoir trimestriellement tous les accès externes
- Superviser spécifiquement l'activité des prestataires

Cartographie des interconnexions

Une cartographie complète doit identifier :

- Tous les points d'interface avec les systèmes externes
- La nature des flux de données échangés
- Les protocoles et mécanismes de sécurité utilisés

- Les dépendances techniques et fonctionnelles
- Les contacts techniques chez chaque partenaire

Cette cartographie sert à :

- Évaluer les risques de propagation d'une attaque
- Identifier les points de défaillance potentiels
- Prioriser les contrôles de sécurité
- Faciliter l'investigation en cas d'incident
- Planifier les tests de sécurité

Gestion des responsabilités

Les responsabilités doivent être clairement définies pour :

- La détection et le signalement des incidents
- Les actions de confinement et remédiation
- La communication en cas de crise
- Les coûts liés à un incident
- La conformité réglementaire
- La continuité de service

Documentation recommandée :

- Matrices RACI pour les différents scénarios d'incident
- Procédures d'escalade inter-organisations
- Coordonnées des contacts d'urgence
- Protocoles de communication de crise
- Plans de continuité coordonnés

Évaluation et prochaines étapes

Comptabilisez vos résultats pour évaluer votre niveau de préparation :

- Nombre de "Oui" : _____ (mesures en place)
- Nombre de "Partiel" : _____ (mesures à finaliser)
- Nombre de "Non" : _____ (mesures à mettre en œuvre)
- Focus sur les éléments prioritaires (*) : nombre de "Non" ou "Partiel" : _____

Niveaux de maturité

En fonction de vos résultats, vous pouvez évaluer votre niveau de maturité :

Niveau initial (0-25% de “Oui”)

- Approche réactive et non structurée
- Risque élevé en cas d’incident
- Besoin urgent d’amélioration sur les fondamentaux

Niveau basique (26-50% de “Oui”)

- Mesures de base en place mais lacunes importantes
- Préparation insuffisante pour des attaques sophistiquées
- Nécessité de structurer et formaliser l’approche

Niveau intermédiaire (51-75% de “Oui”)

- Dispositif solide sur les fondamentaux
- Capacité à gérer des incidents courants
- Besoin d’amélioration sur des aspects spécifiques

Niveau avancé (76-100% de “Oui”)

- Approche mature et proactive
- Bonne préparation aux incidents complexes
- Focus sur l’optimisation et l’amélioration continue

Plan d’action recommandé

1. Commencez par mettre en place les mesures prioritaires (*) manquantes
 - Ces mesures constituent le socle minimum de résilience
 - Leur absence crée des vulnérabilités critiques
 - Leur mise en œuvre apporte des bénéfices immédiats
2. Finalisez les mesures partiellement mises en œuvre
 - Identifiez les blocages et ressources nécessaires
 - Établissez un calendrier réaliste
 - Désignez des responsables pour chaque action

3. Établissez un calendrier pour implémenter les autres mesures

- Priorisez selon les risques spécifiques à votre organisation
- Adoptez une approche progressive et réaliste
- Alignez avec les autres projets et contraintes

4. Réévaluez votre niveau de préparation tous les 6 mois

- Mesurez les progrès accomplis
- Ajustez le plan d'action si nécessaire
- Tenez compte de l'évolution des menaces et de votre organisation

Ressources complémentaires

Organismes de référence

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- National Institute of Standards and Technology (NIST)
- CERT-EU (Computer Emergency Response Team)
- European Union Agency for Cybersecurity (ENISA)

Référentiels utiles

- Guide d'hygiène informatique de l'ANSSI
- Cybersecurity Framework du NIST
- ISO/IEC 27001 (Système de management de la sécurité de l'information)
- SANS Critical Security Controls

Outils d'autoévaluation

- CyberScore de l'ANSSI
- Cyber Resilience Review (CRR) du NIST
- CISA Cyber Resilience Review

Communautés et partage d'information

- Cercles sectoriels de partage (finance, santé, industrie...)
- Dispositifs nationaux d'alerte (CERT)
- Groupes d'utilisateurs des solutions de sécurité

© 2025 Pulse-Crisis - Tous droits réservés