Cyberclean

Les bonnes pratiques de prévention des incidents du SI

Sommaire

Date	Auteur	Observations
06/25/2025	-	-

1) Introduction

Un incident informatique correspond à tout évènement qui perturbent, affectent ou qui peuvent mettre à l'arrêt un système d'information. Il peut s'agir de pannes matérielles / logicielles.
Un incident peut être détecté par un utilisateur (qui va contacter le centre des services) ou par un outil de supervision.

Importance de la prévention des incidents

L'importance de la prévention des incidents pour la disponibilité, la continuité et la sécurité du SI est relativement importante pour la qualité de service et la confiance client notamment.

En effet, dans un contexte d'entreprise comme Cyberclean, la **disponibilité**, c'est à dire l'accès en temps réel aux services numériques peut être affectée par des pannes, des défaillances matérielles ou des erreurs humaines ainsi que la continuité des services sont cruciales pour l'activité de celle-ci. Les serveurs ou autres services doivent être disponibles 24/24 et 7/7.

Prenons l'exemple d'un site internet (celui de Cyberclean), celui-ci doit-être disponible à toute heure afin que les clients ou clients potentiels puissent s'y rendre. Si le site devient inaccessible, même temporairement, cela peut entraîner une baisse de visibilité, des opérations commerciales manquées voire des insatisfactions clients. La prévention des incidents par la surveillance, la redondance ou les alertes en temps réel permet de minimiser les interruptions.

Ensuite, la **continuité** du service fait référence à la capacité de l'entreprise à maintenir ses activités, même en cas de perturbation. Un incident non maîtrisé (comme une attaque par ransomware ou une panne électrique) peut bloquer l'ensemble des opérations.
Des **plans de continuité d'activité (PCA)** et **plans de reprise d'activité (PRA)** doivent donc être prévus pour limiter l'impact sur la productivité et les délais de remise en service.

Enfin, les **incidents de sécurité** (cyberattaques, fuites de données, intrusions) mettent en péril la confidentialité, l'intégrité et la fiabilité des données. Une attaque ciblée sur les serveurs de Cyberclean pourrait non seulement perturber les services, mais aussi causer des dommages d'image et des conséquences juridiques si des données personnelles étaient compromises.

2) Standardisation et sécurisation des postes

La **standardisation des postes** consiste à uniformiser l'environnement informatique utilisé par les collaborateurs de CyberClean : cela inclut le matériel (ordinateurs, imprimantes…), les systèmes d'exploitation, les applications, les configurations réseau et les règles de sécurité. La standardisation s'appuie sur des **modèles d'installation** (images système), des scripts automatisés, et via des stratégies de groupe (GPO).

Standardiser permet un gain de temps pour le déploiement de postes informatiques notamment en s'appuyant sur un master (principe de masterisation).

Avantages

La standardisation permet de :

- Faciliter la maintenance puisque les postes sont soit identiques, soit similaires
- Renforcer la sécurité puisque tous les postes peuvent recevoir les mêmes politiques de sécurité (GPO / antivirus)
- Déployer plus rapidement grâce à l'utilisation d'images systèmes
- Réduire les erreurs humaines : en configurant un poste à la main, des oublis ou des erreurs peuvent être faits, ainsi la standardisation évite ce genre d'erreurs
- Garantir l'homogénéité et la conformité avec les normes internes telle que le RGPD. Cela facilité aussi les audits de sécurité
- Compatibilité logicielle

- Gestion centralisée

Risques en l'absence de standardisation

En l'absence de standardisation, il est possible d'avoir :

- Multiplication des incidents : avec des configurations différentes à chaque poste, les incidents sont plus fréquents. Les problèmes sont alors uniques à chaque machine, ce qui allonge les temps de résolution
- Incohérence au niveau de la sécurité : des mises à jour peuvent être oubliées créant alors des failles de sécurité / vulnérabilités. Aussi, des applications installées manuellement (hors processus) peuvent introduire des risques (ex : logiciel piraté)
- Difficulté pour l'automatisation : en effet, les déploiements (via images systèmes), les sauvegardes ou les politiques de sécurité ne peuvent pas être appliquées de manière homogène
- Incompatibilité logicielle
- Sécurité affaiblie

➡ Pour Cyberclean avec un SI critique la standardisation permet de :

- Garantir la compatibilité avec les logiciels métiers de désinfection et suivi client,
- Réagir rapidement en cas de panne sur un poste utilisateur
- S'assurer que les postes distants soient sécurisés et conformes aux standards de l'entreprise.

Rôle des stratégies de sécurité

Gestion des droits utilisateurs

- Principe du moindre privilège : chaque utilisateur doit disposer uniquement des droits nécessaires à ses tâches.
- Interdiction d'utiliser un compte administrateur local pour une session utilisateur classique.

- Séparation claire entre les comptes utilisateurs standards et comptes techniques.

La mise en place de **GPO** (**Group Policy Object)** est utile pour :

- Restreindre les droits utilisateurs
- Désactiver l'accès aux panneaux de configuration / au système (suivant les utilisateurs)
- Déployer automatiquement des mises à jour et antivirus
- Imposer un mot de passe fort ainsi qu'une durée maximum d'utilisation avant changement
- Configuration de pare-feu Windows et règles de filtrage

Configuration des postes :

- Verrouillage auto après 5 min d'inactivité
- Écran de veille sécurisé : obligation de retaper le mot de passe après verrouillage
- Blocage de la session après 3 ou 5 tentatives (par exemple)

3) Gestion des mises à jour

Les mises à jour servent à corriger les failles de sécurité, déboguer, ajouter ou améliorer des nouvelles fonctionnalités.

Elles sont essentielles pour maintenir la sécurité, la performance et la compatibilité des systèmes d'information. Dans un environnement critique comme celui de CyberClean, une stratégie de gestion centralisée des mises à jour est indispensable pour éviter les failles, les incompatibilités et les interruptions de service.

Stratégie globale de mise à jour

La stratégie de mise à jour doit couvrir l'ensemble des composants du SI :

- OS
- Logiciels tiers : navigateurs, suites bureautiques, etc
- Applications métiers
- Pilotes et firmware

Déploiements des mises à jour

Déploiement automatisé : peut être réalisé à l'aide de Scripts Powershell automatisés ou à l'aide d'outil de gestion centralisée (ex : WSUS). Cela permet :

- Gain de temps (mises à jour réalisées hors période de travail, en heures « creuses »)
- Conformité assurée sur l'ensemble des postes

Déploiement manuel : réservé de préférence pour les postes isolés ou pour des logiciels métiers spécifiques.

Déploiements des mises à jour sur les postes dits nomades (laptops / tablettes).

Ces appareils sont souvent en dehors du réseau interne, donc il est préférable de ne pas effectuer les mises à jour lorsqu'ils ne sont pas dans le réseau mais de les forcer dès la reconnexion au réseau de l'entreprise pour plus de sécurité.

Supervisions des mises à jour

Une fois effectuées, il est nécessaire de surveiller les systèmes post-déploiement. Il est possible d'utiliser des outils de surveillance pour suivre et analyser des éventuels échecs ou problèmes survenus lors des mises à jour ainsi que pour suivre les performance du système après les mises à jour.

Ex : Zabbix (open source)

4) Protection contre les malwares

Solutions logicielles

- Antivirus : l'installation d'un antivirus permet l'identification des logiciels malveillants, la neutralisation des menaces détectées ainsi que l'éradication complète des infections. Son principe : il fonctionne avec une base de données et à chaque nouvelle infection, l'antivirus rentre la signature du virus / malware dans sa base de données. Cela nécessite donc des mises à jour régulières de la base de données.

  Ex : Bitdefender totalsecurity

- Filtrage DNS : il permet d'empêcher aux utilisateurs d'accéder à des sites web malveillants ou contraires à la politique de sécurité de l'entreprise qui peuvent rendre vulnérables l'appareil ou le réseau de l'entreprise.
  Ex : TitanGQ

Méthodes de protection (antivirus) :

- Détection comportementale :
  - Surveillance des activités suspectes
  - Alerte et demande de validation utilisateur
- Analyse heuristique :
  - Examen approfondi du code des programmes
  - Identification des variantes de virus connus
  - Détection des comportements potentiellement malveillants
- Protection Sandbox :
  - Environnement isolé et sécurisé
  - Test des fichiers suspects sans risque
  - Analyse comportementale en temsps réels

Méthodes de remédiation :

- Suppression directe des fichiers infectés
- Réparation des fichiers récupérables
- Isolation en quarantaine pour analyse

Gestion des périphériques amovibles

- Mise en place d'un antivirus / antimalware
- Analyse automatique des clés USB à l'insertion
- Blocage possible par GPO

5) Sauvegardes

Les différents types de sauvegarde :

- Sauvegarde complète : elle consiste à sauvegarder toutes les données d'un ordinateur ou d'un serveur, y compris le système d'exploitation, les bases de données, les applications, les paramètres et les données utilisateur
- Sauvegarde incrémentale : Elle sauvegarde uniquement les données qui ont été modifiées depuis la dernière sauvegarde, qu'elle soit complète ou incrémentale
- Sauvegarde différentielle : Elle sauvegarde toutes les données qui ont été modifiées depuis la dernière sauvegarde complète
- Sauvegarde miroir : Elle crée une copie exacte des données source à chaque exécution

Sauvegarder quoi ?

- Les données (clients / métiers)
- Les configurations systèmes (PC / Switchs / Routeurs / pare feu, etc)
- Les images systèmes (notamment lors de déploiement)

Politique de sauvegarde

Les politiques sauvegardes peuvent être quotidiennes / hebdomadaires / mensuelles ou encore trimestrielles et biannuelles.

Dans le cas de Cyberclean, (ou autre entreprise), des sauvegardes quotidiennes incrémentales ainsi que des sauvegardes complètes hebdomadaires peuvent être envisagées.

Supports

Les sauvegardes peuvent être faites sur :

Disque dur externe

Serveur local ou externe

Site externe
(en cas d'incident dans le bâtiment initial comme un incendie)

Cloud

Rotation des supports

Le principe des sauvegardes sur plusieurs générations (rotation des supports de sauvegarde), consiste à utiliser différents supports de données pour la sauvegarde, ainsi si un support est corrompu, il est possible de retourner à la version de sauvegarde précédente et donc de limiter les pertes.

Test de restauration

Il est essentiel de tester régulièrement la restauration des sauvegardes et l'application d'un plan de continuité ou de reprise d'activité .

Les tests peuvent être mensuels.

Documentation et traçabilité des sauvegardes

La documentation présente :

- Description de la stratégie de sauvegarde mise en place
- Les outils / supports utilisés
- Les fréquences de sauvegardes
- Les responsabilités de chacun
- Procédures de restauration

6) Supervisions et alertes

La supervision permet de détecter rapidement les dysfonctionnements ou anomalies avant qu'ils n'aient un impact significatif, voire d'anticiper des incidents en surveillant des indicateurs clés.

Outils de supervision utilisés

Outil	Fonctionnalités	Commentaire
GLPI + Fusioninventory	Inventaire, supervision simple, alertes de parc	Adapté pour le suivi de matériel et la gestion des incidents
Zabbix	Supervision complète, tableau de bord, alertes avancées	Plus complexe à configurer mais très puissant

Indicateurs à surveiller

Un système de supervision doit pouvoir surveiller les éléments (indicateurs de performance clés) suivant :

- Utilisation CPU des serveurs et postes critiques
- Espace disque disponible (notamment sur les serveurs de fichiers et bases de données)
- Disponibilité réseau (ping, temps de réponse, interruption)
- État des services essentiels (serveur AD, serveur DHCP/DNS, serveur de messagerie…)

- Statut des sauvegardes (réussite, échec, durée)
- Consommation mémoire
- Température des serveurs (notamment si situés dans un environnement sensible)
- Tentatives d'accès échouées (possible indicateur d'attaque ou de mauvaise configuration)

Mises en place d'alertes pertinentes

Les alertes doivent être :

- **Précises** : contenir la nature du problème, le système concerné, et la date/heure
- **Pertinentes** : éviter les faux positifs
- **Hiérarchisées** : critiques (action immédiate), importantes (à traiter), informatives

Exemples d'alertes :

- Espace disque < 10 % sur le serveur de sauvegarde
- Tentative de connexion SSH non autorisée
- Échec de sauvegarde sur 2 jours consécutifs
- Arrêt d'un service critique (AD, base de données métier)

Les alertes peuvent être transmises par :

- Emails
- Intégration à des outils de gestion de tickets (GLPI, OTRS…)

Analyse régulière des journaux d'évènements

L'analyse des logs systèmes permet de comprendre les causes des incidents.

- Sur Windows, l'Observateur d'événements centralise les logs système, sécurité, applications.
- Sur Linux, les logs sont stockés dans /var/log/messages

  Pour voir en temps réel les derniers évènements qui y sont écrits, écrire : **tail -f /var/log/messages**

7) Télé-dépannage et interventions à distance

Le télédépannage permet de :

- Gagner du temps (pas de déplacement physique)
- Réagir plus rapidement aux incidents
- Maintenir une continuité de service, même à distance
- Gérer les interventions sur les postes nomades

Outils autorisés et sécurisation des accès

Outils	Fonctionnalités	Sécurité
AnyDesk	Accès distant rapide, portable	Chiffrement Aes-256, mot de passe pour l'accès
RustDesk (open source)	Alternative à TeamViewer	Auto-hébergement possible
SSH (linux / serveurs)	Contrôle à distance par ligne de commande	Authentification par clés

Outils pour démarrage PXE pour dépannage / installation

Le démarrage PXE (Preboot eXecution Environment) permet de démarrer un poste sur le réseau pour :

- Réinstaller un OS
- Lancer une image de diagnostic
- Effectuer une récupération système

Exemples de cas d'usage

- Un poste ne démarre plus (OS corrompu)
- Déploiement d'une image système standardisée

Outil : FOG Project

Gestion des identifiants d'accès distants

Il existe plusieurs éléments essentiels pour sécuriser les accès distants en s'assurant que seuls les utilisateurs autorisés peuvent accéder aux ressources nécessaires et ce, de manière sécurisée. Les éléments sont les suivants :

- Gestion du cycle de vie des identités : création, mise à jour et suppression des identités numériques des utilisateurs, qu'ils soient humains ou non humains
- Contrôle d'accès : définition et application de politiques d'accès précises pour s'assurer que les utilisateurs disposent uniquement des permissions nécessaires à leurs fonctions.
- Authentification et autorisation : processus de vérification de l'identité des utilisateurs et de détermination de leurs droits d'accès aux ressources.
- Gouvernance des identités : surveillance et audit des activités des utilisateurs pour garantir la conformité aux politiques de sécurité et aux réglementations.

8) Sensibilisation des utilisateurs finaux

Sensibilisation des utilisateurs et préventions des incidents

La sensibilisation des utilisateurs est essentielle dans la prévention des incidents car ils sont souvent la première cause d'une faille. Leur sensibilisation et leur formation sont essentielles pour la protection des données.

Les sensibilisation peuvent porter sur les attaques telles que le phishing (par le biais de mails ou SMS frauduleux), les ransomwares ou d'autres logiciels malveillants.

Types incidents causés par des erreurs humaines ou négligences utilisateurs

- Clic sur un lien frauduleux (phishing)
- Téléchargement d'un fichier infecté
- Connexion à un Wi-Fi public sans VPN
- Partage involontaire de fichiers confidentiels
- Utilisation de mots de passe faibles ou réutilisés

Actions concrètes renforçant la culture de la cybersécurité chez Cyberclean

Action	Objectif
Campagnes internes de sensibilisation ex : email, affiches	Rappeler les bonnes pratiques de façon régulière
Formations courtes (en présentiel ou non)	Expliquer les menaces actuelles et rappeler les bonnes pratiques
Test de Phishing (au sein de l'entreprise)	Tester les réactions des salariés / utilisateurs face à des attaques réelles
Newsletter	Diffuser les actualités de sécurité et bonnes pratiques
Intégration au livret d'accueil	Sensibiliser les nouveaux arrivants

Mesurer l'efficacité d'une campagne de sensibilisation

- Taux de réussite aux tests (ex : test de phishing)
- Feedback via questionnaire anonyme
- Check du nombre d'incidents utilisateurs signalés

Intégration de la sensibilisation dans l'accueil des nouveaux collaborateurs

Il est possible d'intégrer la sensibilisation sur la sécurité informatique dans l'accueil des nouveaux collaborateurs via des livrets contenant la charte informatique, les règles d'usages et outils numériques ainsi que les comportements à éviter / interdits.

Il est aussi possible de l'intégrer via une formation obligatoire dès l'arrivé d'un ou des nouveaux collaborateurs.

9) Conclusion

L'adoption de bonnes pratiques et de procédures claires, partagées par tous, est essentielle pour assurer la qualité et la cohérence du travail. La documentation des processus renforce l'efficacité, réduit les erreurs et facilite l'intégration. Pour rester performante, l'organisation doit aussi s'inscrire dans une logique d'amélioration continue en réévaluant régulièrement ses méthodes et en impliquant ses équipes.

10) Sources

> https://www.atlassian.com/fr/incident-management#the-importance-of-incident-management

> https://aws.amazon.com/fr/what-is/incident-management/

> https://www.intel.fr/content/www/fr/fr/business/enterprise-computers/resources/os-image-deployment.html

> Une plus grande standardisation de l'infrastructure informatique

> Comment appliquer une GPO sur un groupe spécifique ?

> Maîtriser les GPO : Un guide complet pour une gestion efficace du réseau

> BBe Cours 2024 Impress

> Les sauvegardes - Notions et pratique (VM).pdf

> Surveillance du réseau - Zabbix

> Wazuh - Open Source XDR. SIEM open source.

> TUTOS.EU : Afficher les logs sous Linux

> Qu'est-ce que la gestion des identités et des accès (IAM) ? | IBM

> Sécurité : Impliquer et former les utilisateurs | CNIL