04/04/2025

SAE44 – Cyber

Livrable final

Aliya M. et Sarah Sivani PONNU
BUT2 RESEAUX ET TELECOMMUNICATIONS – GROUPE 2

Table des matières

Partie 1 : Politique de Sécurité des Systèmes d'Information (PSSI) – RecycloTech

A. Introduction

La Politique de Sécurité des Systèmes d'Information (PSSI) est un document fondamental pour toute organisation souhaitant protéger ses actifs informationnels, maîtriser les risques liés à l'usage des technologies numériques, et garantir la continuité de ses activités. Chez RecycloTech, jeune entreprise innovante spécialisée dans le recyclage de matériel électronique, le système d'information constitue un pilier stratégique de l'activité. L'usage de plateformes numériques pour la gestion logistique, la traçabilité, la vente en ligne, la relation client ou encore le traitement des flux financiers rend impératif l'encadrement rigoureux de l'ensemble des processus liés à la sécurité informatique.

La PSSI vise ainsi à définir un cadre organisationnel, technique et humain permettant de protéger les ressources numériques, tout en assurant une utilisation conforme, efficace et maîtrisée des technologies. Elle s'adresse à l'ensemble des collaborateurs, prestataires et partenaires disposant d'un accès aux ressources numériques de l'entreprise. Elle constitue à la fois un socle de référence et un levier d'amélioration continue de la posture de cybersécurité de RecycloTech.

La présente politique est alignée avec les normes et bonnes pratiques internationales, telles que la norme ISO/IEC 27001 relative à la gestion de la sécurité de l'information, les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), ainsi qu'avec les obligations légales imposées par le Règlement Général sur la Protection des Données (RGPD).

B. Contexte

RecycloTech est une entreprise de 50 collaborateurs répartis sur plusieurs pôles métiers, dont une équipe informatique composée de techniciens et d'ingénieurs spécialisés en cybersécurité, réseaux, infrastructure, développement web et support. La société œuvre dans un secteur particulièrement sensible : le traitement, le reconditionnement et la revente de matériel informatique. Ce positionnement stratégique implique la manipulation d'un volume conséquent de données personnelles, techniques, commerciales et parfois confidentielles, qu'il est crucial de protéger.

Le système d'information de RecycloTech est constitué d'un ensemble d'équipements et de services critiques, incluant un site web marchand, un portail B2B à destination des entreprises, un ERP interne, des bases de données clients, des serveurs applicatifs, des postes utilisateurs, et des solutions de communication et de collaboration en ligne. Ce système est exposé à divers risques : attaques par ransomware, phishing, compromission d'identifiants, fuites de données,

erreurs humaines, etc. En conséquence, la sécurité des systèmes d'information est une priorité stratégique portée au plus haut niveau de l'organisation.

La complexité croissante de l'environnement numérique, combinée à la montée en puissance des menaces cyber, impose une structuration solide, cohérente et dynamique de la politique de sécurité. Celle-ci ne doit pas être perçue comme une contrainte mais comme un moyen de garantir la pérennité des activités, de renforcer la confiance des clients et partenaires, et de répondre de manière proactive aux évolutions réglementaires et technologiques.

C. Responsabilités

La sécurité du système d'information repose sur une répartition claire des responsabilités entre les différents acteurs de l'organisation. La Direction Générale de RecycloTech assume la responsabilité globale de la sécurité et en délègue l'exécution à la Direction des Systèmes d'Information et de la Sécurité (DSSI).

Le DSSI est en charge de la définition de la politique, de sa mise en œuvre, de son contrôle et de son évolution. Il coordonne l'ensemble des équipes informatiques et s'assure de l'application homogène des mesures de sécurité à tous les niveaux du système d'information.

Au sein de la DSSI, différents pôles assument des responsabilités spécifiques :

- **Le pôle cybersécurité** identifie les menaces, évalue les risques, met en œuvre les mesures de protection, organise les audits internes et coordonne la réponse aux incidents.

- **Le pôle infrastructure** gère les serveurs, les services cloud, la virtualisation, la politique de sauvegarde, et le maintien en condition de sécurité des systèmes.

- **Le pôle réseaux et télécommunications** garantit la connectivité sécurisée des sites, la segmentation des réseaux, l'accès distant sécurisé, et le bon fonctionnement des équipements réseau.

- **Le pôle développement web** développe et maintient les applications métier, le portail e-commerce et les outils internes, en veillant à intégrer des pratiques de développement sécurisé (DevSecOps).

- **Le pôle support utilisateurs** intervient en assistance directe auprès des collaborateurs, gère les incidents techniques du quotidien, et contribue à la sensibilisation aux bonnes pratiques de sécurité.

Chaque collaborateur est également acteur de la sécurité. L'usage du système d'information est encadré par une charte informatique signée à l'embauche, qui précise les obligations de chacun en matière d'accès, de confidentialité, de protection des données et d'utilisation des ressources numériques. Le non-respect de ces règles peut entraîner des sanctions disciplinaires, conformément au règlement intérieur de l'entreprise.

D. Objectifs de sécurité

La politique de sécurité de RecycloTech est construite autour des trois piliers fondamentaux de la sécurité de l'information :

1. **Confidentialité** : garantir que seules les personnes habilitées peuvent accéder aux données sensibles. Cela concerne particulièrement les données clients, les informations financières, les contrats commerciaux et les configurations techniques critiques. Toute fuite ou consultation non autorisée de ces données peut entraîner des conséquences juridiques, financières et réputationnelles graves.
2. **Intégrité** : s'assurer que les données et les systèmes ne sont pas modifiés de manière non autorisée, volontairement ou par erreur. Le maintien de l'intégrité est essentiel pour garantir la fiabilité des rapports, des diagnostics, des stocks et des transactions.
3. **Disponibilité** : veiller à ce que les utilisateurs puissent accéder aux services et aux données dont ils ont besoin pour travailler, même en cas d'incident technique ou de cyberattaque. Cela implique une redondance des services critiques, une sauvegarde régulière et des procédures de reprise d'activité éprouvées.

Ces objectifs sont traduits dans des plans d'action concrets, mesurables et régulièrement réévalués. La sécurité n'est pas une fin en soi, mais un levier pour permettre à l'entreprise de fonctionner de manière efficace, résiliente et conforme aux attentes de ses parties prenantes.

E. Contrôles de sécurité

Afin d'atteindre les objectifs de sécurité précités, RecycloTech déploie une combinaison de contrôles techniques, organisationnels et humains adaptés aux risques identifiés.

1. Contrôles techniques

Les systèmes sont protégés par des dispositifs de sécurité éprouvés :

- L'authentification forte est imposée sur les comptes à privilèges et les accès distants.
- Les flux de données sont chiffrés via des protocoles sécurisés (HTTPS, TLS 1.3, VPN IPSec).
- Des pares-feux filtrent le trafic entrant et sortant aux différentes frontières du réseau.
- Les antivirus et solutions EDR surveillent en temps réel les comportements suspects sur les postes et serveurs.
- Un plan de patching régulier permet de corriger les vulnérabilités connues.
- Une supervision permanente est assurée via des outils comme Zabbix, Grafana et des sondes de sécurité.

2. Contrôles organisationnels

Des procédures internes définissent les modalités d'accès, les règles de gestion des incidents, les plans de sauvegarde, les modalités d'onboarding et d'offboarding des utilisateurs, ainsi que les processus de validation des changements techniques.

Les profils utilisateurs sont définis selon le principe du moindre privilège : chaque collaborateur dispose uniquement des droits strictement nécessaires à l'exercice de ses missions.

3. Contrôles humains

La sensibilisation des utilisateurs fait l'objet d'une attention constante. Des campagnes d'information, des modules de formation, des rappels réguliers sur les bonnes pratiques permettent d'ancrer une culture de la sécurité. L'humain étant souvent le maillon faible, il est aussi le premier rempart face aux attaques sociales.

F. Gestion des incidents

RecycloTech a mis en place une procédure formelle de gestion des incidents de sécurité, articulée autour des étapes suivantes : détection, qualification, confinement, résolution, et retour d'expérience.

La détection repose sur des outils de supervision technique, mais également sur le signalement humain. Tout utilisateur est encouragé à signaler tout comportement ou message suspect.

Lorsqu'un incident est détecté, la cellule de crise cybersécurité est activée. Elle est composée du DSSI, du RSSI, d'un administrateur système, d'un responsable réseau et, si nécessaire, d'un représentant de la direction générale. Une analyse rapide est menée pour identifier l'origine de l'incident, mesurer son impact, et mettre en œuvre des mesures de confinement.

Une fois l'incident résolu, un rapport détaillé est rédigé, incluant une analyse des causes profondes, les mesures correctrices mises en œuvre, et les recommandations pour éviter une récurrence. Ce retour d'expérience est partagé avec les parties concernées et intégré dans l'amélioration continue de la PSSI.

G. Sensibilisation à la sécurité

La protection du système d'information passe aussi par une appropriation collective des enjeux de cybersécurité. RecycloTech considère la sensibilisation comme un levier stratégique.

Tous les nouveaux collaborateurs suivent une formation d'intégration incluant une séquence sur la sécurité informatique. Chaque année, une campagne de sensibilisation thématique est

organisée (ex. : mois européen de la cybersécurité, cybermois). Des quizz, ateliers interactifs, et simulations de phishing sont utilisés pour renforcer l'engagement.

Des rappels réguliers sont effectués : newsletters cybersécurité, affiches de rappel dans les locaux, messages sur l'intranet. Cette pédagogie de terrain vise à faire de chaque utilisateur un acteur responsable, capable d'adopter les bons réflexes face aux menaces.

H. Revue et amélioration

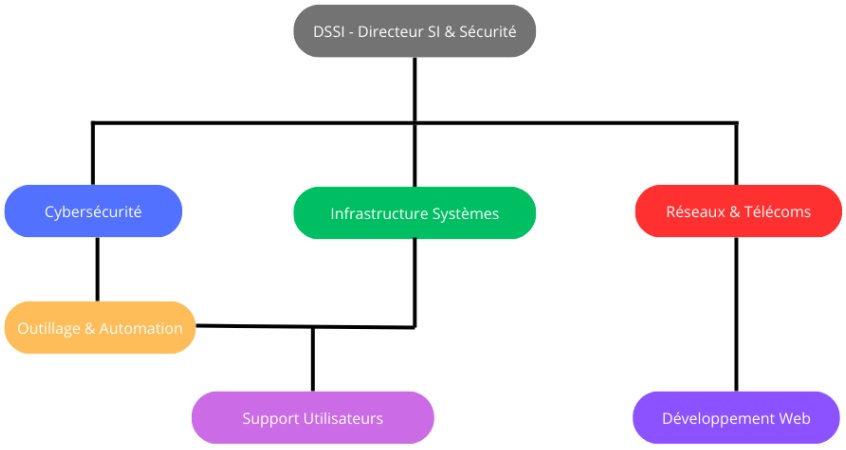
La PSSI est un document vivant, qui doit évoluer avec les risques, les technologies, les usages, et les exigences réglementaires. RecycloTech procède à une revue annuelle de la politique, pilotée par la DSSI et impliquant les responsables de chaque pôle informatique. En cas d'incident majeur ou de modification structurelle du SI, une mise à jour exceptionnelle peut être déclenchée.

L'amélioration continue est favorisée par :

- La veille technologique et réglementaire
- L'analyse des incidents passés
- Les résultats des audits internes
- Les retours des utilisateurs

Cette dynamique d'adaptation permanente permet à RecycloTech de maintenir un haut niveau de sécurité, en phase avec l'évolution de ses activités et de son écosystème.

Organigramme du pôle informatique :



L'organigramme ci-dessous illustre la structure du département informatique de RecycloTech. Il met en évidence à la fois les relations hiérarchiques entre les pôles, ainsi que les interactions

fonctionnelles transverses. Les lignes verticales indiquent une relation hiérarchique directe entre le DSSI (Directeur des Systèmes d'Information et de la Sécurité) et les différents pôles techniques. Quant aux connexions latérales (branches), elles montrent que certains services sont partagés ou coopèrent étroitement.

Par exemple, le pôle "Outillage & Automation" est rattaché à l'infrastructure, en fournissant des outils d'automatisation et de supervision. Le pôle "Support utilisateurs", quant à lui, est transversal : il est en interaction avec tous les autres pôles pour assurer un service fluide aux collaborateurs. Cette organisation permet à l'entreprise d'être agile et de mutualiser certaines compétences pour gagner en efficacité, tout en gardant une structure claire et fonctionnelle.

Partie 2 : Procédure de Patching – Serveurs de production RecycloTech

A. Introduction générale

La gestion des correctifs de sécurité (ou "patch management") constitue l'un des piliers fondamentaux de la cybersécurité opérationnelle. Elle permet de corriger les vulnérabilités connues, de réduire la surface d'attaque des systèmes et d'anticiper les compromissions liées à des failles non corrigées. Chez RecycloTech, la mise à jour régulière des serveurs de production s'inscrit dans une stratégie globale de maintien en condition de sécurité (MCS) du système d'information.

Dans un contexte où les menaces évoluent rapidement et où de nouvelles failles sont découvertes chaque jour (ex. : CVE Zero-Day), l'application rapide et maîtrisée des correctifs permet de garantir la résilience des infrastructures, de respecter les bonnes pratiques recommandées par les agences de sécurité (ANSSI, CERT-FR, CISA), et de maintenir un haut niveau de disponibilité des services numériques critiques. Cette procédure documente en détail le processus de patching déployé chez RecycloTech.

B. Évaluation des correctifs

La première étape consiste à surveiller et identifier les mises à jour de sécurité publiées par les éditeurs de logiciels, les constructeurs de matériel et les communautés open-source. Le pôle cybersécurité effectue une veille hebdomadaire à l'aide de plusieurs sources fiables : bulletins du CERT-FR, flux CVE, portails des éditeurs (Microsoft, Debian, Red Hat), et forums spécialisés.

Chaque mise à jour détectée est évaluée selon plusieurs critères :

- Criticité de la vulnérabilité (CVSS)
- Surface d'exposition (serveur interne vs exposé Internet)
- Potentiel d'exploitation active (exploits disponibles dans Metasploit, GitHub, etc...

- Compatibilité avec l'environnement existant
- Impact potentiel sur la continuité de service

Cette analyse est réalisée à l'aide d'un tableau de priorisation, alimenté en continu. L'outil GLPI, connecté à l'inventaire des actifs via FusionInventory, permet d'identifier rapidement les systèmes concernés et d'évaluer leur exposition.

Des cas particuliers peuvent être identifiés, comme les mises à jour de sécurité urgentes (ex. : failles critiques "wormables" comme EternalBlue), qui sont alors traitées en procédure accélérée.

C. Planification des correctifs

Une fois les correctifs identifiés et qualifiés, la planification constitue une étape essentielle pour assurer un déploiement sans interruption majeure. RecycloTech a mis en place des fenêtres de maintenance régulières, généralement en dehors des horaires de bureau (soirée ou week-end), selon les contraintes de chaque service.

La planification est organisée selon plusieurs principes :

- Information préalable des utilisateurs via l'intranet et le support
- Coordination avec les équipes métiers en cas de dépendance applicative
- Disponibilité des équipes techniques (astreinte ou rotation)
- Vérification préalable des sauvegardes avant toute intervention

Certains services critiques disposant de haute disponibilité (cluster, redondance) peuvent être patchés en rolling update, sans interruption visible pour les utilisateurs. Dans d'autres cas, un basculement temporaire sur des serveurs de secours est prévu (disaster recovery plan light).

Le calendrier mensuel des patchs est validé par le DSSI et partagé avec l'ensemble des pôles IT.

D. Test des correctifs

La politique de sécurité de RecycloTech impose que tout correctif soit testé en environnement de préproduction avant d'être appliqué en production. Cette étape vise à vérifier :

- L'intégrité des services après installation
- L'absence d'erreur système ou applicative
- La compatibilité avec les versions des bibliothèques logicielles ou pilotes
- Le bon redémarrage des services critiques

L'environnement de préproduction est maintenu à l'identique de la production : mêmes versions logicielles, mêmes configurations, données fictives anonymisées. Ce clonage régulier permet de simuler les patchs dans des conditions réelles.

Les tests sont réalisés en suivant un scénario de validation fonctionnelle, rédigé par les administrateurs système et validé par le référent applicatif concerné. En cas de

dysfonctionnement, un rapport de non-conformité est ouvert, et l'application du patch est suspendue.

E. Déploiement des correctifs

Lorsque les tests sont concluants, les correctifs sont déployés selon un processus automatisé, sécurisé et tracé. Le pôle infrastructure utilise principalement les outils suivants :

- Ansible pour le patching Linux (Debian, Ubuntu, CentOS)
- WSUS pour les mises à jour Windows Server
- Scripts PowerShell signés pour les correctifs spécifiques
- Playbooks YAML versionnés dans Git pour la traçabilité

Les opérations sont supervisées en temps réel et les éventuelles erreurs remontées dans la console centrale. Chaque patch appliqué est consigné dans un journal de maintenance incluant :

- La date d'intervention
- Le système ciblé
- Le nom du correctif (KB ou CVE)
- Le responsable technique
- L'état de validation post-patching

F. Vérification et validation

Une fois les correctifs déployés, une phase de vérification post-patching est systématiquement lancée. Elle inclut :

- Vérification des versions logicielles via scripts d'audit
- Contrôle de l'état des services via systemctl, Get-Service, ou supervision Zabbix
- Test de l'interface utilisateur (portail web, accès aux fichiers, etc.)
- Vérification des logs d'erreurs applicatifs et systèmes

Récupération de la charge CPU/Mémoire/IO disque pour vérifier les effets de bord

Cette validation est réalisée par un administrateur différent de celui qui a effectué le patching, dans un souci de double contrôle. Le résultat est notifié dans un rapport de conformité validé par le pôle cybersécurité.

G. Gestion des exceptions

Dans certains cas, un patch peut ne pas être appliqué immédiatement. Cela peut se produire lorsqu'un correctif :

- Présente un bug connu non encore corrigé
- Est incompatible avec une application métier critique
- Nécessite une interruption de service inacceptable à court terme

Dans ces situations, une demande d'exception doit être formalisée et validée par le DSSI. Elle inclut :

- La justification technique et fonctionnelle
- Le risque identifié
- Le plan de contournement temporaire (ex : limitation d'accès, isolation réseau)
- La date prévisionnelle de correction

Les exceptions sont réévaluées tous les mois et suivies dans un registre dédié, en lien avec la cartographie des risques.

H. Suivi, documentation et amélioration continue

L'ensemble des opérations de patching est intégré dans le processus d'amélioration continue de la sécurité. Des indicateurs sont suivis en continu :

- Taux de serveurs patchés dans les 30 jours
- Nombre de correctifs critiques non appliqués
- Délai moyen de déploiement entre détection et installation
- Nombre d'exceptions actives

Ces indicateurs alimentent le tableau de bord cybersécurité, présenté chaque trimestre au comité technique IT. Les données sont historisées dans GLPI et exportées vers des outils de reporting internes (Grafana, Power BI).

Chaque année, une revue complète de la stratégie de patching est réalisée : nouveaux outils, procédures améliorées, retours d'expérience, nouveaux standards (Zero Trust, micro-segmentation, etc.).

Partie 3 : Durcissement des systèmes avec AppLocker – Cas d'étude au sein de RecycloTech

A. Contexte et stratégie de l'entreprise

Dans un contexte de cybermenaces croissantes, RecycloTech place la sécurité des postes de travail au cœur de sa stratégie de protection des systèmes d'information. En effet, chaque terminal constitue un point d'entrée potentiel pour les attaquants. Un simple clic sur un fichier malveillant, un téléchargement non autorisé, ou l'exécution d'un script détourné peut suffire à

compromettre tout ou partie de l'environnement numérique de l'entreprise. C'est dans ce cadre que le projet de durcissement des postes de travail a été initié.

L'un des enjeux majeurs identifiés par le pôle cybersécurité de RecycloTech réside dans la limitation des libertés d'exécution applicative sur les systèmes Windows. La multiplication des logiciels malveillants (ransomwares, logiciels espions, chevaux de Troie) mais aussi l'usage détourné d'outils natifs comme PowerShell, mshta.exe ou rundll32.exe (les LOLBins) expose les organisations à des attaques sophistiquées exploitant leurs propres systèmes contre elles-mêmes.

Pour répondre à ces menaces, RecycloTech a retenu la solution AppLocker, une fonctionnalité native des systèmes Windows professionnels et entreprise. AppLocker permet de restreindre l'exécution des logiciels sur la base de règles administratives, selon plusieurs critères : l'éditeur (signature), le chemin d'accès, le hachage du fichier ou encore le type de fichier (EXE, script, DLL...).

Cette approche repose sur une logique de "whitelisting applicatif", où seules les applications expressément autorisées peuvent s'exécuter. L'objectif est ainsi de réduire drastiquement la surface d'attaque tout en maintenant un environnement de travail fluide et cohérent pour les utilisateurs finaux.

AppLocker s'inscrit pleinement dans la stratégie de durcissement du SI de RecycloTech, aux côtés du patching, de la segmentation réseau, de l'authentification forte et de la supervision. Le projet a démarré par un projet pilote structuré, centré sur une unité d'organisation dédiée et un utilisateur test.

B. Préparation du projet pilote

Avant de généraliser le déploiement d'une stratégie AppLocker à l'ensemble des collaborateurs, RecycloTech a opté pour une phase pilote structurée. Cette phase a permis d'évaluer les impacts potentiels, de valider la faisabilité technique et d'impliquer les acteurs métiers concernés.

1. Objectifs du pilote

Avant de généraliser AppLocker à l'ensemble des postes de travail, une phase expérimentale contrôlée a été mise en œuvre. Cette étape avait pour objectifs :

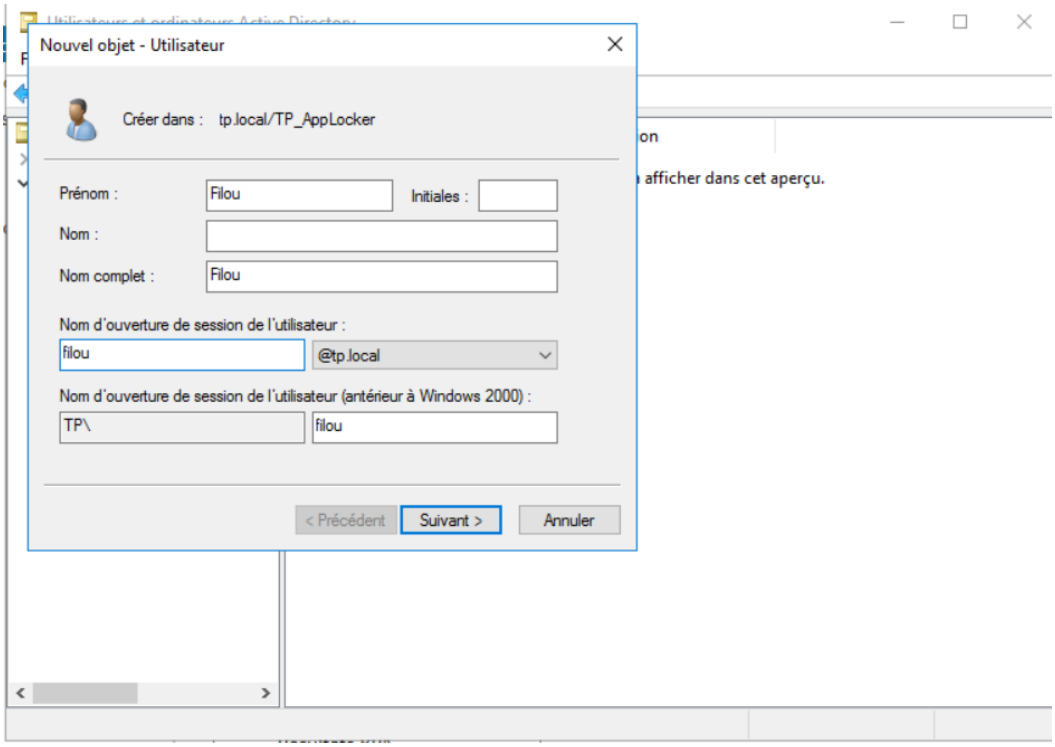
- De tester l'efficacité du blocage d'exécutables non autorisés sur les postes Windows ;
- De valider la compatibilité des règles avec les logiciels métiers utilisés au quotidien (navigateur, messagerie, outils bureautiques...) ;
- De superviser les événements générés par AppLocker pour s'assurer de leur traçabilité
- De préparer le déploiement progressif, en définissant une méthode reproductible et acceptable pour les utilisateurs.

Ce projet pilote a permis d'identifier les limites techniques, les contraintes opérationnelles, mais aussi les gains en termes de sécurité, avant un éventuel passage à l'échelle.

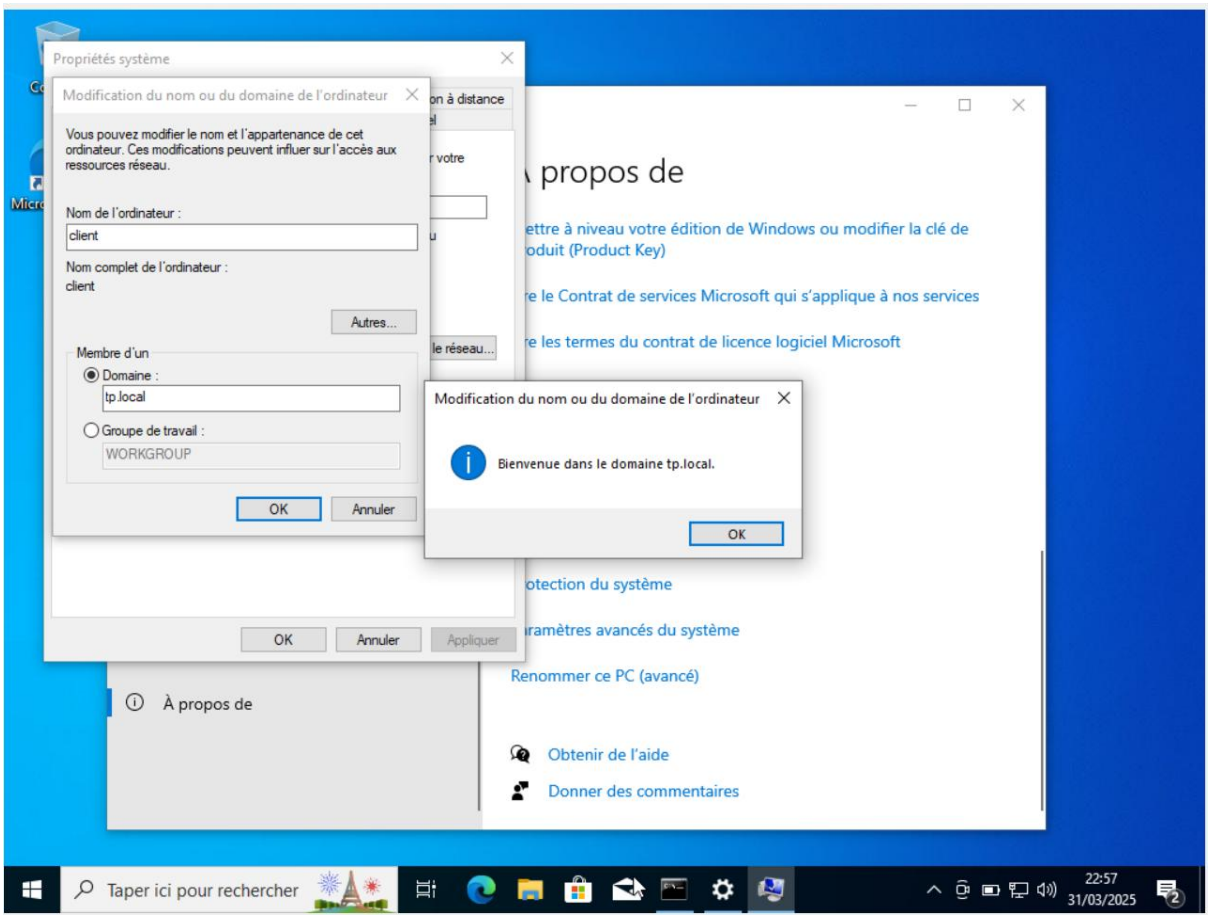
2. Environnement de test

Le test s'est déroulé dans un environnement réseau représentatif, isolé de la production. Il comprenait :

- Un contrôleur de domaine sous Windows Server 2016, hébergeant Active Directory, la gestion des GPO et le serveur DNS ;
- Une unité d'organisation (OU) nommée TP_AppLocker, spécifiquement créée pour héberger le poste de test ;
- Un poste client Windows 10 Professionnel proprement intégré au domaine ;
- Un utilisateur standard nommé "Filou", créé dans Active Directory pour simuler l'environnement d'un collaborateur classique.



Cette capture montre l'ajout du compte utilisateur "Filou" dans l'OU dédiée au projet AppLocker.



Le poste de test est bien rattaché au domaine tp.local, ce qui permet l'application centralisée des GPO.

Le compte utilisateur "Filou" ne dispose d'aucun droit particulier : il est membre du groupe Utilisateurs du domaine, ce qui garantit un périmètre d'exécution limité. Le poste client a été fraîchement installé et configuré selon les normes internes : antivirus à jour, supervision active, et accès aux outils de bureautique courants.

C. Déploiement et configuration des règles AppLocker

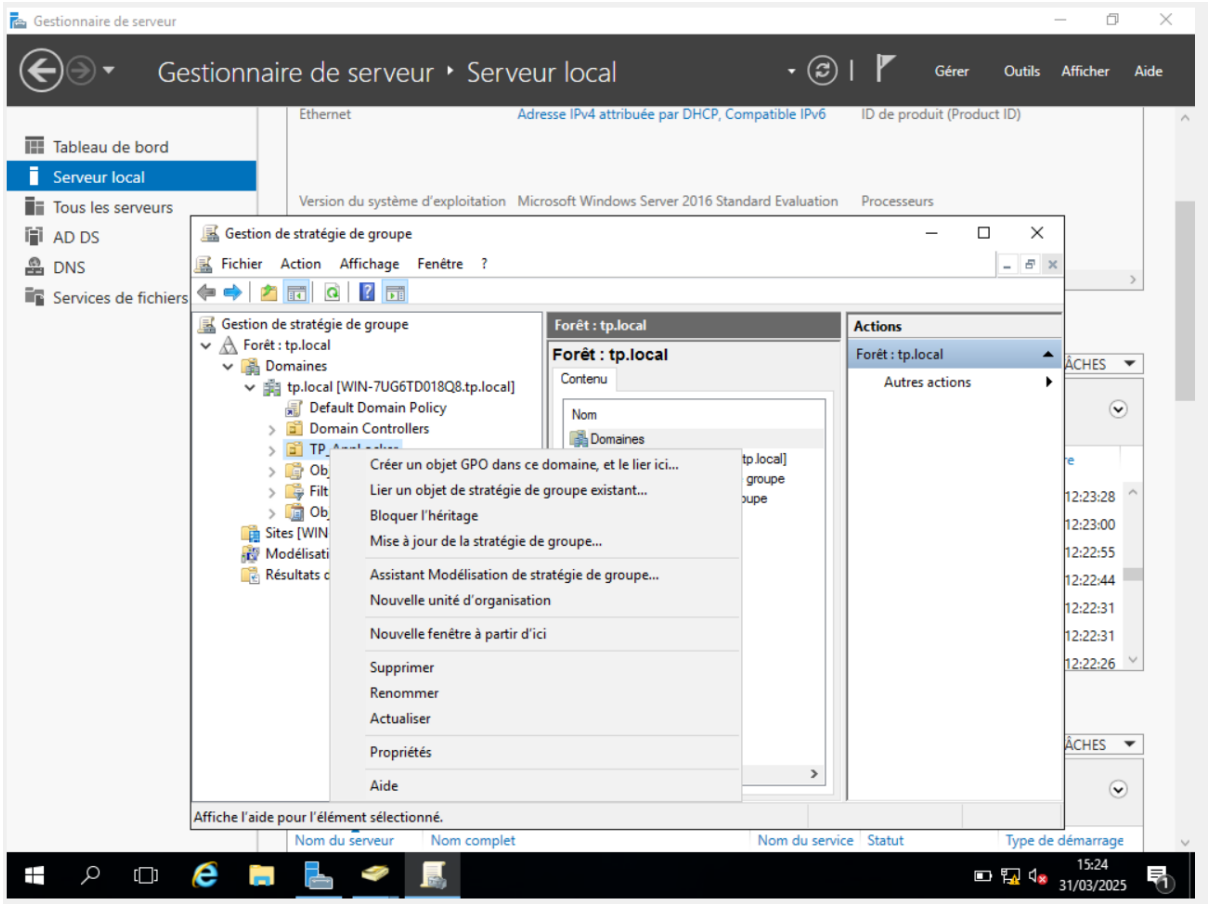
L'activation d'AppLocker a été réalisée via une stratégie de groupe (GPO) liée à l'OU de test. Celle-ci a été configurée pour interdire explicitement certaines applications tout en autorisant celles nécessaires au fonctionnement normal du poste.

1. Création de la stratégie AppLocker

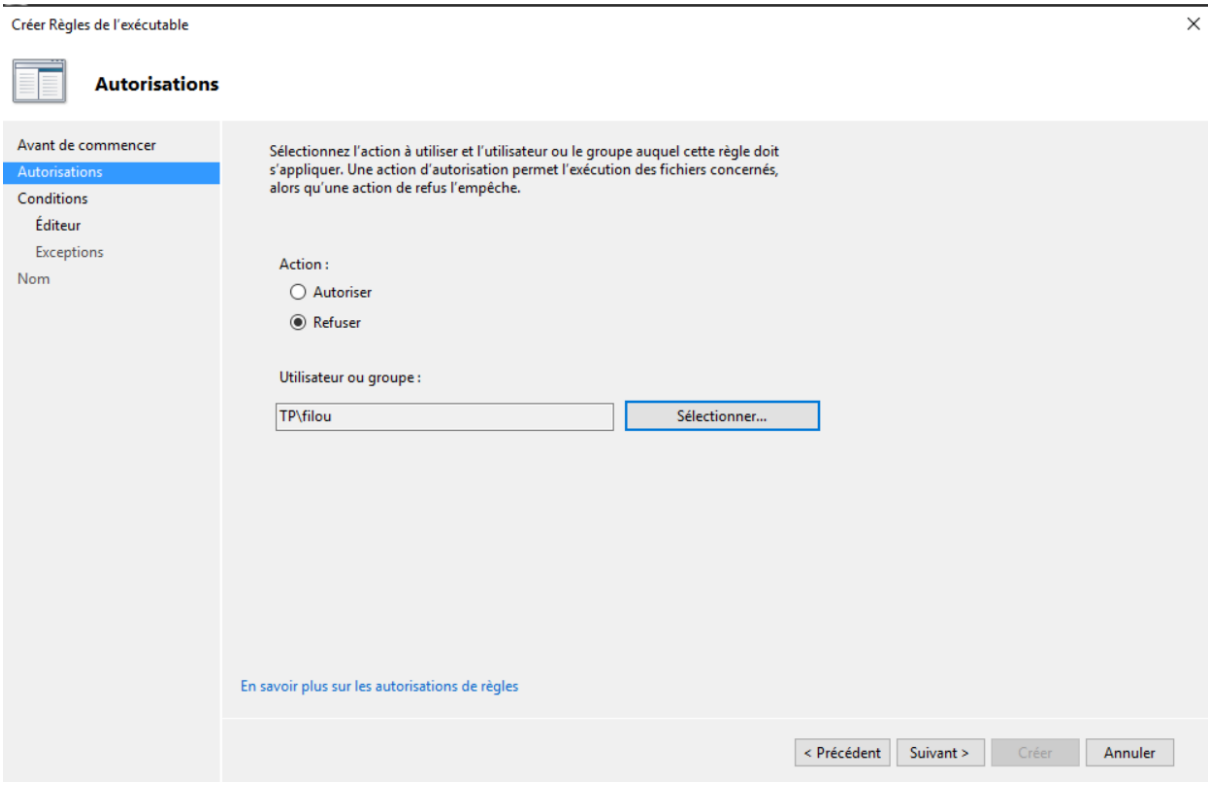
La première étape du déploiement consiste à créer une stratégie de groupe dédiée. Une GPO nommée AppLocker_TestFilou a été créée sur le contrôleur de domaine, puis liée à l'OU contenant le poste de test.

Dans cette stratégie :

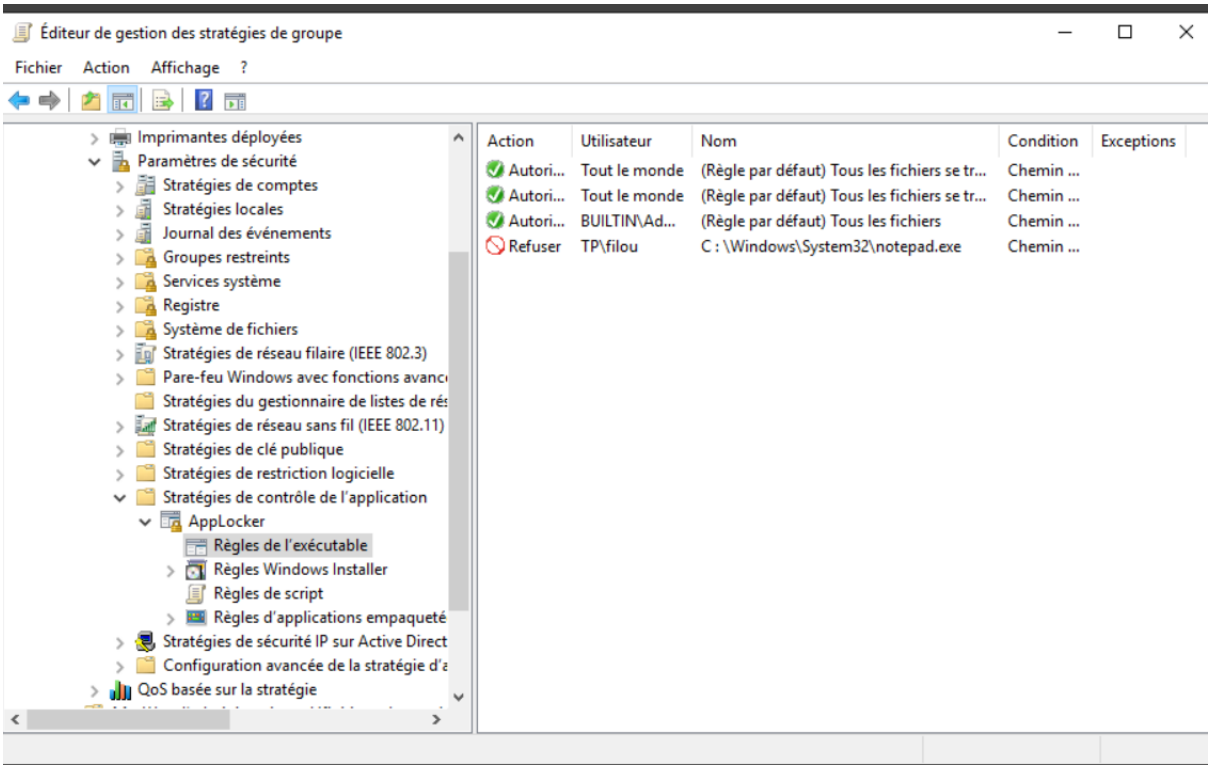
- Le service "Application Identity" est activé, condition indispensable au fonctionnement d'AppLocker ;
- Les règles par défaut sont générées automatiquement : elles permettent l'exécution de tous les fichiers système Windows signés par Microsoft (dans C:\Windows et C:\Program Files) ;
- Une règle personnalisée est ajoutée manuellement pour interdire le lancement de Notepad (notepad.exe) pour l'utilisateur "Filou".



La stratégie est appliquée uniquement à l'unité d'organisation contenant le poste et l'utilisateur de test.



La stratégie est appliquée uniquement à l'unité d'organisation contenant le poste et l'utilisateur de test.



L'interface d'AppLocker permet de cibler un utilisateur spécifique et d'interdire l'exécution d'un binaire précis.

2. Validation fonctionnelle

À la reprise de session, l'utilisateur "Filou" tente d'ouvrir Notepad via l'explorateur de fichiers. Immédiatement, un message d'erreur s'affiche, indiquant que "cette application a été bloquée par l'administrateur système". Cela confirme que la règle AppLocker a bien été appliquée et empêche désormais l'exécution de l'exécutable ciblé.

Dans le même temps, les autres applications essentielles (navigateur, Outlook, explorateur de fichiers, suite bureautique) continuent de fonctionner normalement. Cela démontre que la politique appliquée est suffisamment ciblée pour bloquer une application spécifique sans perturber l'environnement de travail global.

D. Enjeux de déploiement à l'échelle

À l'issue de la phase pilote, les retours ont été majoritairement positifs. L'utilisateur de test a confirmé que la politique n'impactait pas son activité. L'équipe technique a pu vérifier que le mécanisme fonctionnait sans provoquer d'instabilité. Sur cette base, un déploiement progressif à l'ensemble des utilisateurs a été envisagé.

1. Stratégie de généralisation

- Extension à l'ensemble des comptes non techniques (comptabilité, logistique)
- Déploiement aux postes critiques (RH, direction)
- Durcissement progressif avec des règles par éditeur ou hachage
- Bascule en mode "renforcement" (après une phase d'observation passive)

Chaque étape est précédée d'un audit applicatif, d'un test pilote sur 5 à 10 postes, et d'un point de validation avec les équipes concernées.

2. Limites et précautions

AppLocker présente toutefois certaines limitations :

- Fonctionne uniquement sur les éditions professionnelles ou Entreprise de Windows
- Peut être contourné si mal configuré (exécution dans chemins non filtrés, comme %Temp%)
- Ne couvre pas tous les langages de script (par défaut, PowerShell n'est que partiellement limité)
- Pour pallier ces limites, RecycloTech prévoit d'étudier l'intégration de WDAC (Windows Defender Application Control) à plus long terme, en parallèle du renforcement de l'EDR.

Partie 4 : Gestion de crise – Simulation d'une attaque ciblée sur RecycloTech

A. Contexte de l'entreprise et exposition au risque

RecycloTech, entreprise technologique en plein essor spécialisée dans le recyclage et la revalorisation de matériel informatique, s'appuie largement sur des outils numériques pour assurer ses activités logistiques, commerciales et relationnelles. Avec plus de 50 collaborateurs, une plateforme e-commerce, un portail B2B et une infrastructure d'information centralisée, elle manipule quotidiennement des données sensibles : informations personnelles de clients, identifiants d'accès, inventaires de matériels reconditionnés, données de facturation, et historiques d'intervention.

Comme toute entreprise numérique, RecycloTech est exposée à de nombreux risques cyber. En particulier :

- Phishing ciblé via ingénierie sociale
- Infiltration via prestataires tiers ou sous-traitants
- Propagation de ransomware par rebond réseau
- Compromission de comptes utilisateurs mal protégés

Failles applicatives dans le site e-commerce ou les services exposés

Le risque cyber n'est plus théorique : chaque faille peut être exploitée par des attaquants motivés, organisés, ou automatisés via des campagnes massives. C'est pourquoi l'entreprise a décidé de tester sa capacité de réaction à travers une simulation de crise réaliste, construite autour d'un scénario de ransomware.

B. Scénario de crise retenu : infection par ransomware suite à un mail piégé

Le scénario imaginé est volontairement simple mais redoutablement crédible. Il reproduit un cas fréquent dans les PME et ETI françaises : l'ouverture d'un fichier piégé transmis par email, menant à l'exécution d'un ransomware.

1. Déroulé du scénario

Un employé du service comptabilité, récemment recruté, reçoit un email en apparence légitime, envoyé par une adresse ressemblant à celle d'un client habituel. L'objet du message est pressant : "Facture en attente – URGENT". Le corps de l'email contient un message poli, une fausse signature, et une pièce jointe nommée facture_urgent2024.exe.

Le fichier est en réalité un exécutable déguisé en PDF. Lors de son ouverture, un ransomware s'installe en arrière-plan. En moins de 5 minutes :

- Les fichiers locaux sont chiffrés
- Le malware se propage via les partages réseau accessibles en lecture/écriture
- Des fichiers avec l'extension .locked apparaissent
- Une note de rançon est déposée sur chaque répertoire : "Vos fichiers ont été chiffrés. Pour les récupérer, payez en Bitcoin à l'adresse suivante..."

Le logiciel de supervision Zabbix détecte un pic d'activité anormal sur le protocole SMB. Plusieurs utilisateurs signalent ne plus pouvoir ouvrir leurs documents. L'alerte est déclenchée.

C. Déclenchement et coordination de la cellule de crise

1. Détection initiale

Le premier signal est donné par un utilisateur du service logistique, qui appelle le support pour signaler une erreur à l'ouverture d'un fichier Excel. Le technicien constate que le fichier est corrompu, et que plusieurs autres présentent des extensions inconnues. En parallèle, Zabbix enregistre une activité réseau inhabituelle : transfert massif de fichiers via SMB entre plusieurs postes internes.

Le technicien de support escalade immédiatement l'incident au RSSI, qui en informe le DSSI. Celui-ci déclenche la cellule de crise cybersécurité dans les 30 minutes suivant l'incident.

2. Composition de la cellule

- DSSI : coordination générale de la crise
- RSSI : analyse de la menace, pilotage technique
- Administrateur système : confinement des machines, récupération des sauvegardes
- Administrateur réseau : isolation VLAN, filtrage des flux suspects
- Responsable communication : gestion des messages internes et externes
- Représentant de la direction : prise de décision stratégique

3. Canaux de communication

Un canal Teams privé est immédiatement créé, baptisé "CRISE CYBER – 4 avril 2025". Les communications par email sont suspendues, sauf pour les envois officiels. Un document de suivi partagé est ouvert pour centraliser les informations en temps réel (logins impactés, machines infectées, actions menées...).

D. Réponse opérationnelle et remédiation

La cellule de crise adopte une stratégie structurée, suivant les étapes standard de gestion d'incident : confinement, investigation, remédiation, restauration.

1. Confinement rapide

- Isolement réseau des postes infectés via VLAN de quarantaine
- Désactivation temporaire de l'accès VP
- Blocage des partages de fichiers (Samba, SMBv1 désactivé)
- Recherche de fichiers ".locked" sur les serveurs partagés
- Interruption temporaire du site e-commerce par précaution

La propagation est stoppée après environ 2 heures d'intervention.

2. Investigation technique

Les administrateurs identifient le point d'entrée : le poste d'un utilisateur non formé, sans filtrage renforcé. Les journaux révèlent que le fichier malveillant a été exécuté avec les droits utilisateurs, mais a profité d'un accès aux dossiers partagés pour chiffrer un grand volume de données.

La version du ransomware est reconnue comme une variante de LockBit, exploitant un mécanisme de chiffrement asymétrique. Les notes de rançon ne laissent entrevoir aucune possibilité de récupération sans la clé privée.

3. Restauration et remédiation

Heureusement, les serveurs les plus critiques disposent de snapshots journaliers. Après vérification de l'intégrité des sauvegardes, les restaurations sont lancées :

- Serveur de fichiers partagé → restauration à J-1
- ERP → retour à l'état stable précédant l'attaque
- Postes infectés → reformatés et réinstallés via une image ISO contrôlée

Les mots de passe administrateur sont changés, un scan antivirus complet est lancé, et les logs de connexion sont analysés pour repérer d'éventuelles intrusions secondaires.

E. Communication interne et externe

Dans le cadre d'un incident de sécurité, la communication constitue un axe stratégique à part entière, complémentaire des actions techniques de réponse. Une gestion efficace de la communication permet de limiter la propagation d'informations inexactes, de maintenir la confiance des utilisateurs internes, de rassurer les partenaires externes, et de préparer les éléments de langage en cas de publication publique ou de fuite d'information. Chez RecycloTech, l'activation de la cellule de crise s'accompagne automatiquement de la mise en œuvre d'un plan de communication de crise coordonné par un responsable désigné.

1. Communication interne

Dès les premières heures de la crise, une communication claire, transparente et structurée est adressée à l'ensemble des collaborateurs. L'objectif est d'informer sans provoquer de panique, tout en fournissant les consignes immédiates à respecter. Un premier message, envoyé via Teams et affiché sur l'intranet interne, indique qu'un incident de sécurité est en cours, que certaines ressources sont momentanément indisponibles, et que des équipes spécialisées sont mobilisées pour rétablir la situation dans les meilleurs délais.

Dans un second temps, un message signé par la direction générale et la DSSI est diffusé à tous les collaborateurs. Celui-ci rappelle le contexte de l'incident, souligne l'origine probable (fichier malveillant ouvert par inadvertance), et insiste sur les bonnes pratiques à adopter dans les heures et jours suivants : ne pas ouvrir de pièces jointes suspectes, signaler tout comportement anormal sur les postes, respecter les consignes données par le support.

Par ailleurs, une réunion d'information est organisée en visioconférence avec les responsables de pôles. Elle permet de faire un point d'étape plus détaillé, de répondre aux questions, de rassurer les équipes et d'expliquer les mesures en cours de déploiement (restauration des services, vérification des accès, changement de mots de passe...).

Cette communication interne vise également à éviter la diffusion de rumeurs ou de versions erronées de l'événement. Elle fait partie intégrante de la gestion de la crise, en favorisant une mobilisation collective, une compréhension des enjeux, et un alignement des comportements. Le ton utilisé reste professionnel mais humain, assumant l'incident tout en valorisant la réactivité des équipes.

2. Communication externe

Sur le plan externe, la posture de communication doit être mesurée, anticipée et adaptable à la gravité réelle ou potentielle de l'incident. Dans le cas de cette simulation, aucun élément ne laisse penser qu'une fuite de données ait eu lieu. Toutefois, une communication préventive est préparée par précaution. Un brouillon de communiqué de presse est rédigé en amont, prêt à être publié dans le cas où une atteinte à la confidentialité des données devait être confirmée.

Ce communiqué inclut les éléments suivants : la date de l'incident, la nature de l'attaque, les services impactés, les mesures mises en œuvre pour contenir la menace, les actions prises pour rétablir les systèmes, et l'engagement de l'entreprise à renforcer ses dispositifs de

cybersécurité. Le ton reste factuel, sans dramatisation, mais démontre la transparence et la responsabilité de l'entreprise.

Parallèlement, le DPO (Délégué à la Protection des Données) est alerté dès les premières heures. Il évalue, avec l'équipe juridique et le RSSI, si une déclaration auprès de la CNIL est nécessaire. Conformément au RGPD, toute violation de données à caractère personnel doit en effet être notifiée dans un délai de 72 heures, si elle est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

Les clients professionnels (partenaires B2B), quant à eux, sont directement contactés par les chargés de comptes via un message personnalisé. Ce message les informe que des lenteurs ou interruptions temporaires ont pu être observées, sans entrer dans les détails techniques de l'incident, et les rassure sur le fait qu'aucune compromission de leurs données n'est actuellement confirmée. Cette démarche proactive permet de préserver la relation commerciale, en montrant que l'entreprise agit avec rigueur et transparence.

Enfin, une veille sur les réseaux sociaux est activée afin de détecter toute fuite d'information, tentative de désinformation ou commentaire public lié à l'incident. Le responsable communication se tient prêt à intervenir rapidement en cas de besoin, avec des messages pré-rédigés validés par la direction.

F. Rétablissement progressif des services

Après deux jours d'effort intensif, l'ensemble des services critiques est à nouveau opérationnel. Le site e-commerce est remis en ligne, les utilisateurs récupèrent progressivement l'accès à leurs dossiers et outils.

Des mesures immédiates de renforcement sont prises :

- Blocage de l'exécution des .exe dans les dossiers utilisateurs
- Déploiement de la MFA sur les accès distants
- Mise à jour du client EDR sur l'ensemble des postes
- Ajout de règles AppLocker renforcées

G. Retour d'expérience (REX) et enseignements

Une fois la crise passée, la cellule rédige un rapport complet d'incident, incluant :

- Chronologie de l'attaque
- Liste des systèmes impactés
- Mesures prises et leur efficacité
- Enseignements techniques et organisationnels

1. Leçons principales

- La vigilance utilisateur est essentielle : la formation et les tests de phishing doivent être renforcés.
- L'isolement rapide du réseau a été décisif pour éviter une propagation plus large.
- La qualité des sauvegardes a permis un rétablissement rapide.
- L'absence d'un plan de réponse formalisé a entraîné une certaine confusion au démarrage.

2. Améliorations prévues

- Mise à jour du plan de réponse à incident
- Rédaction d'une fiche réflexe "Ransomware"
- Réalisation de simulations de crise régulières
- Création d'un guide de communication de crise