Ruben Battocchio
20/01/2026

TP CH4-TD2

I. Introduction

Contexte : À la demande de M. Brillat, une veille informationnelle doit être mise en place concernant les mises à jour et les correctifs logiciels (patchs) du système d'exploitation Windows.

Objectifs identifiés : Pour répondre à ce besoin, la veille doit permettre de :

1. Anticiper les menaces : Détecter la publication de nouvelles failles de sécurité (CVE) affectant Windows avant qu'elles ne soient exploitées.
2. Planifier la maintenance : Être informé des dates de sortie des mises à jour officielles (notamment le "Patch Tuesday" de Microsoft) pour organiser les déploiements sans gêner la production.
3. Vérifier la fiabilité : Identifier les retours d'expérience sur ces mises à jour (bugs potentiels, incompatibilités) avant de les installer sur tout le parc informatique.

II. Identifier les qualifications et ressources numériques

Type de ressource	Rapidité d'accès	Fiabilité	Actualité	Pertinence (Windows)	Qualification
Sites Officiels & Newsletters (Microsoft Security Response Center, ANSSI)	Moyenne (Validation requise)	**Très Haute**	Haute	**Maximale**	**Source indispensable** (Source primaire fiable).
Flux RSS / Sites Tech spécialisés (ZDNet, TheVerge, ITConnect)	**Haute**	Haute	**Très Haute**	Haute	**Excellente** pour une veille quotidienne automatisée.
Réseaux Sociaux (Twitter/X - Experts cybersécurité)	**Immédiate**	Variable (Risque de rumeur)	Temps réel	Moyenne (Beaucoup de "bruit")	Utile pour les alertes "Zero-day" mais **à vérifier**.

Forums & Communautés (Reddit Sysadmin, Microsoft Answers)	Moyenne	Basse (Avis utilisateurs)	Moyenne	Variable	Utile pour le **dépannage**, pas pour l'alerte.

III. Tratégie de diffusion des informations

Une fois l'information collectée et analysée, elle doit être transmise aux bonnes personnes.

1. Les Cibles :

- M. Brillat (DSI) : Pour les décisions stratégiques et budgétaires.
- L'équipe technique (Admins système) : Pour l'application technique des patchs.
- Les utilisateurs finaux : Uniquement en cas de menace critique nécessitant de la vigilance (ex: campagne de phishing ou redémarrage forcé).

2. Canaux et Supports de communication :

- Alerte Critique (Immédiat) :
  - *Canal :* Email avec mention "URGENT" + Messagerie instantanée (Teams/Slack).
  - *Support :* Bulletin d'alerte court (Nature de la faille, Risque, Action requise).
- Veille Régulière (Hebdomadaire) :
  - *Canal :* Réunion de service du lundi ou Email récapitulatif.
  - *Support :* Note de synthèse (comme celle demandée au TD précédent). Elle résume les mises à jour de la semaine (Patch Tuesday), les correctifs testés et le planning de déploiement.
- Base de connaissances :
  - *Canal :* Intranet ou outil de ticket.
  - *Support :* Archivage des procédures de mise à jour pour référence future.

IV. Conclusion

Ce travail de préparation a permis de structurer une démarche de veille informationnelle rigoureuse, indispensable à la sécurité du système d'information de l'entreprise.

En sélectionnant des sources primaires fiables comme l'ANSSI ou le Centre de sécurité Microsoft , et en utilisant un agrégateur de flux performant comme Feedly (retenu pour son efficacité face au volume d'informations), nous sommes désormais capables de :

1. Centraliser l'information dispersée sur le web.
2. Filtrer le bruit pour ne retenir que les alertes pertinentes pour notre environnement Windows.
3. Diffuser rapidement les actions correctives aux équipes techniques.

Cette organisation permettra à l'entreprise de passer d'une gestion réactive des incidents à une gestion proactive des vulnérabilités, réduisant ainsi considérablement les risques d'attaques informatiques.