La politique de sécurité

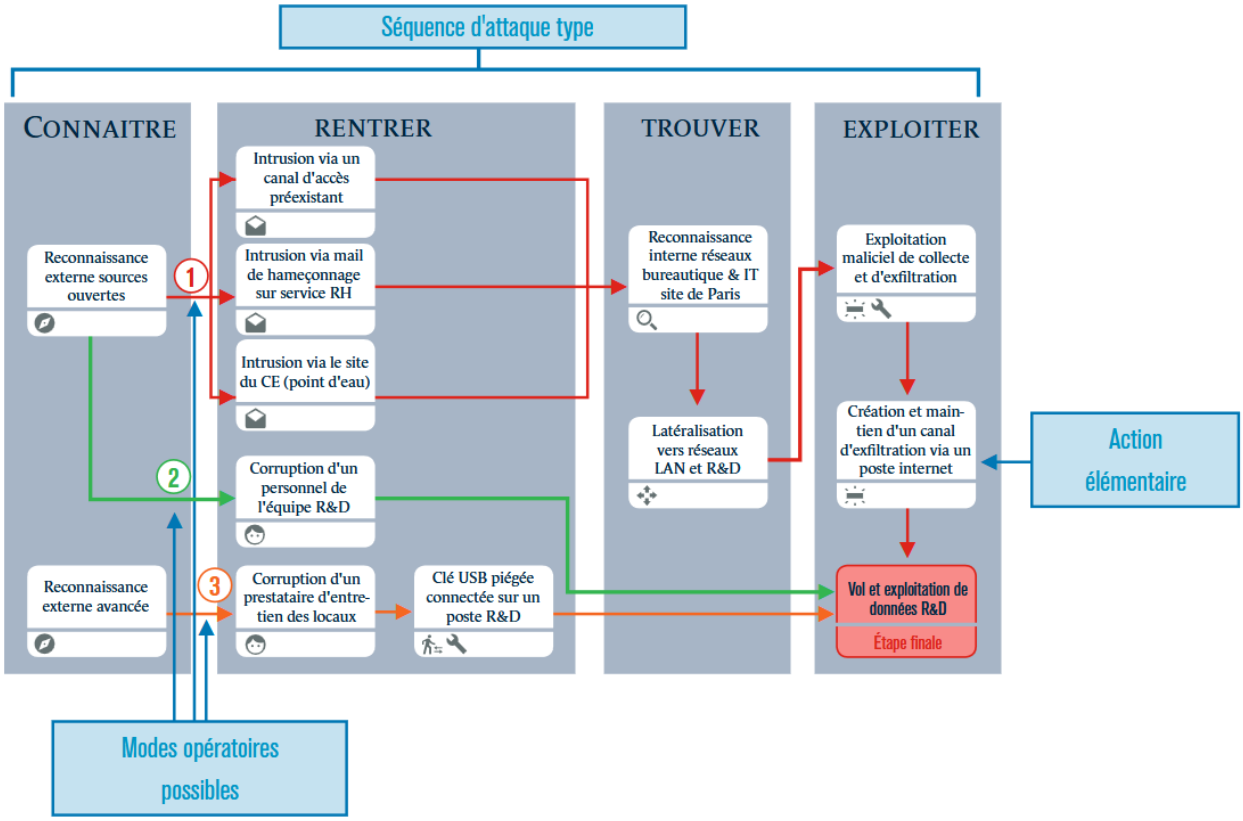
1 – Définitions

Politique de sécurité	Ensemble de règles pour protéger : ✓ Les données ✓ Les systèmes ✓ Les utilisateurs

OBJECTIF
Éviter les accès non autorisés
Protéger contre les attaques
Garantir CIA (Confidentialité, Intégrité, Disponibilité)

Scenario d'attaque

La meilleure façon de concevoir une politique de sécurité est d'analyser la méthode d'attaque d'un pirate. L'exemple suivant propose trois modes opératoires.



Une séquence d'attaque s'articule autour de quatre phases :

CONNAITRE → Collecte d'informations
RENTRER → Intrusion dans le système
TROUVER → Recherche des données
EXPLOITER → Vol ou destruction des données

Les éléments essentiels d'une politique de sécurité

- **Identification des actifs**
  Recenser les actifs informatiques de l'organisation : données, applications, équipements, etc.

- **Gestion des accès**
  Définir les règles d'accès aux ressources informatiques, mots de passe forts, double authentification, etc.

- **Sensibilisation à la sécurité**
  Formation des employés → éviter le phishing, les erreurs humaines, etc.

- **Gestion des risques :**
  Identifier les failles liées à la sécurité informatique et mettre en place des mesures pour les atténuer.

- **Gestion des incidents**
  Élaborer un plan d'intervention en cas d'incident : détecter, réagir et restaurer.

Exemple simplifié d'une politique de sécurité pour une petite organisation

Cet exemple présente un extrait de la politique de sécurité d'une organisation à travers 10 points importants. Voici un résumé.
Texte en rouge : idées à développer et à adapter en fonction de l'organisation.

Politique de Sécurité de l'Information

1. Objectif
L'objectif de cette politique est de protéger les informations sensibles de l'entreprise contre tout accès non autorisé, divulgation ou destruction. On peut ajouter du matériel spécifique, des locaux, …

2. Champ d'Application
Cette politique s'applique à tous les employés, consultants, contractuels et partenaires ayant accès aux systèmes et données de l'entreprise.

3. Responsabilités
- **Direction** : Responsable de la mise en œuvre et du respect de cette politique.
- **Responsable de la Sécurité (RSSI)** : Chargé de la gestion quotidienne de la sécurité et de la conformité à cette politique.
- **Employés** : Doivent suivre les procédures de sécurité et signaler tout incident ou violation.
  On peut différencier certaines parties des employés en fonction de leur niveau d'accréditation, de leur géolocalisation, etc.

4. Contrôle d'Accès
- **Accès aux Systèmes** : L'accès aux systèmes informatiques est limité aux utilisateurs autorisés.
- **Gestion des Mots de Passe** : Les mots de passe doivent être complexes et changés tous les 90 jours.
- **Authentification Multi-Facteurs** : Utilisée pour accéder aux systèmes sensibles.
  On peut préciser les types d'accès (physique ou logique), les caractéristiques des mots de passes, les type d'authentification autorisé ou pas.

5. Sécurité des Réseaux
- **Pare-feu** : Tous les réseaux doivent être protégés par des pare-feu.
- **VPN** : Utilisation obligatoire pour les connexions à distance.
  On peut lister tous les appareils qui participent à la sécurisation du réseau, les spécificités du VPN (type de serveur, local à l'entreprise ou privé, etc), le type de chiffrage.

6. Gestion des Incidents
- **Signalement** : Tout incident de sécurité doit être signalé immédiatement au responsable de la sécurité.
- **Réponse** : Une équipe dédiée est responsable de la gestion des incidents et de la restauration des services.
  On peut préciser les protocoles à suivre en cas d'incident, la reprise après incident, etc.

7. Formation et Sensibilisation

- **Formation Initiale** : Tous les nouveaux employés reçoivent une formation sur les politiques de sécurité.
- **Sensibilisation Régulière** : Des sessions de sensibilisation sont organisées chaque trimestre.
  On peut préciser les notions abordées lors des formations, etc.

8. Surveillance et Audit

- **Surveillance** : Les systèmes sont surveillés en continu pour détecter les activités suspectes.
- **Audit** : Des audits de sécurité sont réalisés annuellement.
  On peut préciser le type de matériel utilisé, le type de données analysées, etc.

9. Conformité

- **Réglementations** : La politique est conforme aux réglementations locales et internationales (ex. : RGPD).
- **Révision** : La politique est révisée annuellement pour s'assurer de son efficacité et de sa pertinence.

10. Sanctions

- **Non-Respect** : Tout manquement à cette politique peut entraîner des sanctions disciplinaires, y compris le licenciement.
  On peut lister les différentes sanctions, etc.