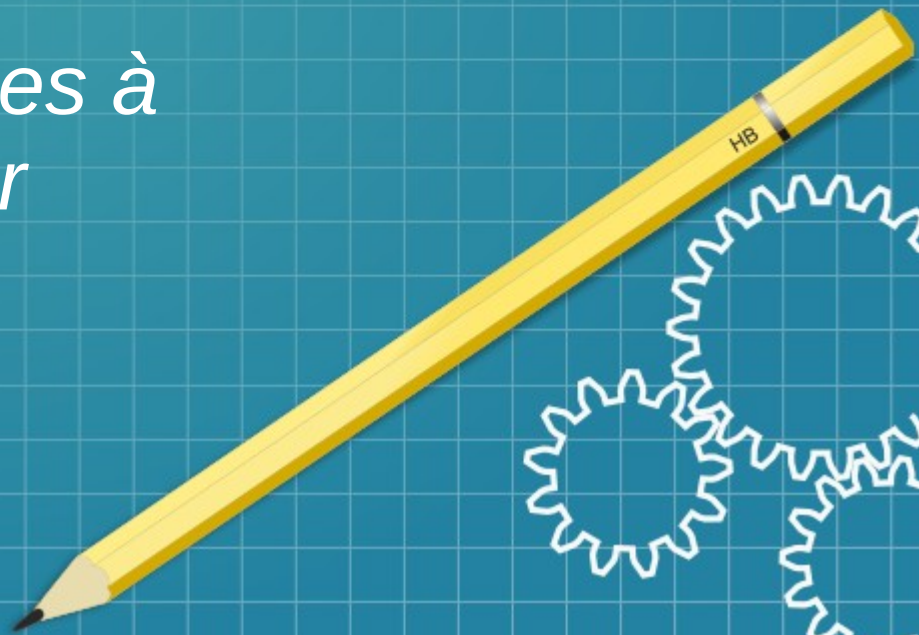
Politique d’entreprise :
la sécurité informatique

Les dix règles à observer



1) Mettre en place une politique

Consiste pour l'entreprise à créer un document comportant toutes les règles de sécurité du système d'information, avec :

- Les bonnes pratiques de sécurité de la téléphonie, du web et de la messagerie électronique
- Les règles concernant le téléchargement et/ou l'installation de nouveaux logiciels
- Comment bien choisir ses mots de passe, etc.
- L'audit du système informatique et de ses vulnérabilités avec par exemple :

Les test d'intrusion font partie de l'audit technique. Ils se divisent en tests « boite blanche » (avec toutes les informations techniques), les tests « boite grises » (avec un compte utilisateur) et les tests « boite noire » (en condition réelle de hacking).

2) Sensibiliser le personnel

La sensibilisation des collaborateurs aux risques de la cybercriminalité est primordiale ; Il faut donc éduquer les employés.

<u>Exemples de risque :</u>

- Utilisation d'une clé USB « oubliée » sur un bureau
- Réponse à un email sans vérification de l'émetteur
- Etc…

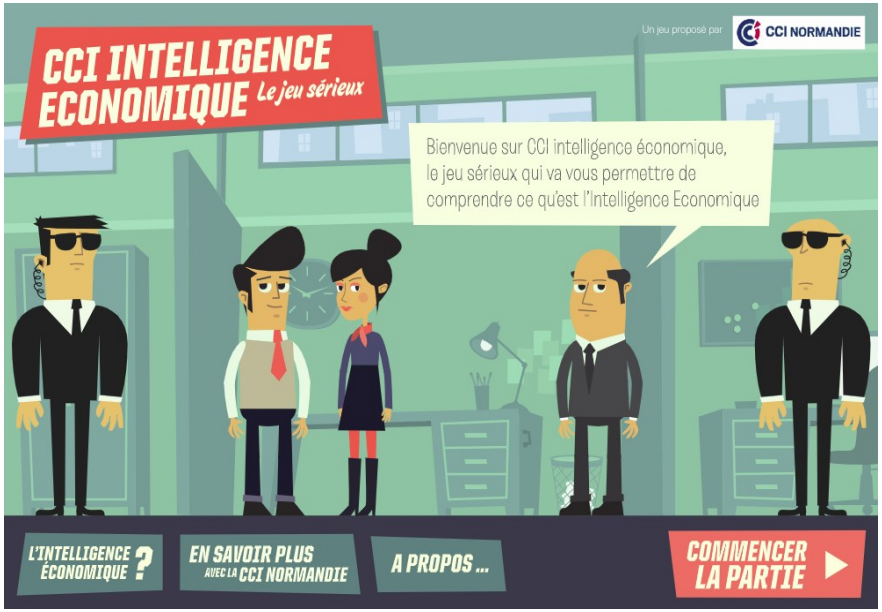
Supports de formation possibles :

→ https://www.cybermalveillance.gouv.fr/

pour les dispositifs d'assistance fournis

par le gouvernement

→ Jeu sérieux http://www.jeu-ie.cci.fr/

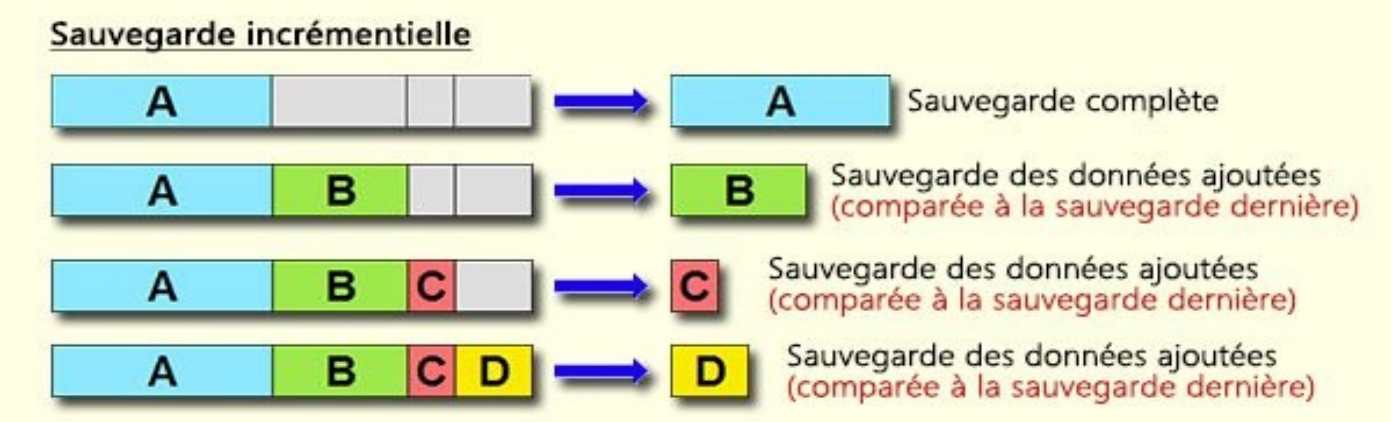


3) Sauvegarder les données

Le patrimoine numérique d'une société est le socle de son activité. Les données capitales d'une entreprise doivent être centralisées et sauvegardées quotidiennement sur un serveur local (pour plus de contrôle) et distant en cas de sinistres physiques (vols/incendies/intempéries).

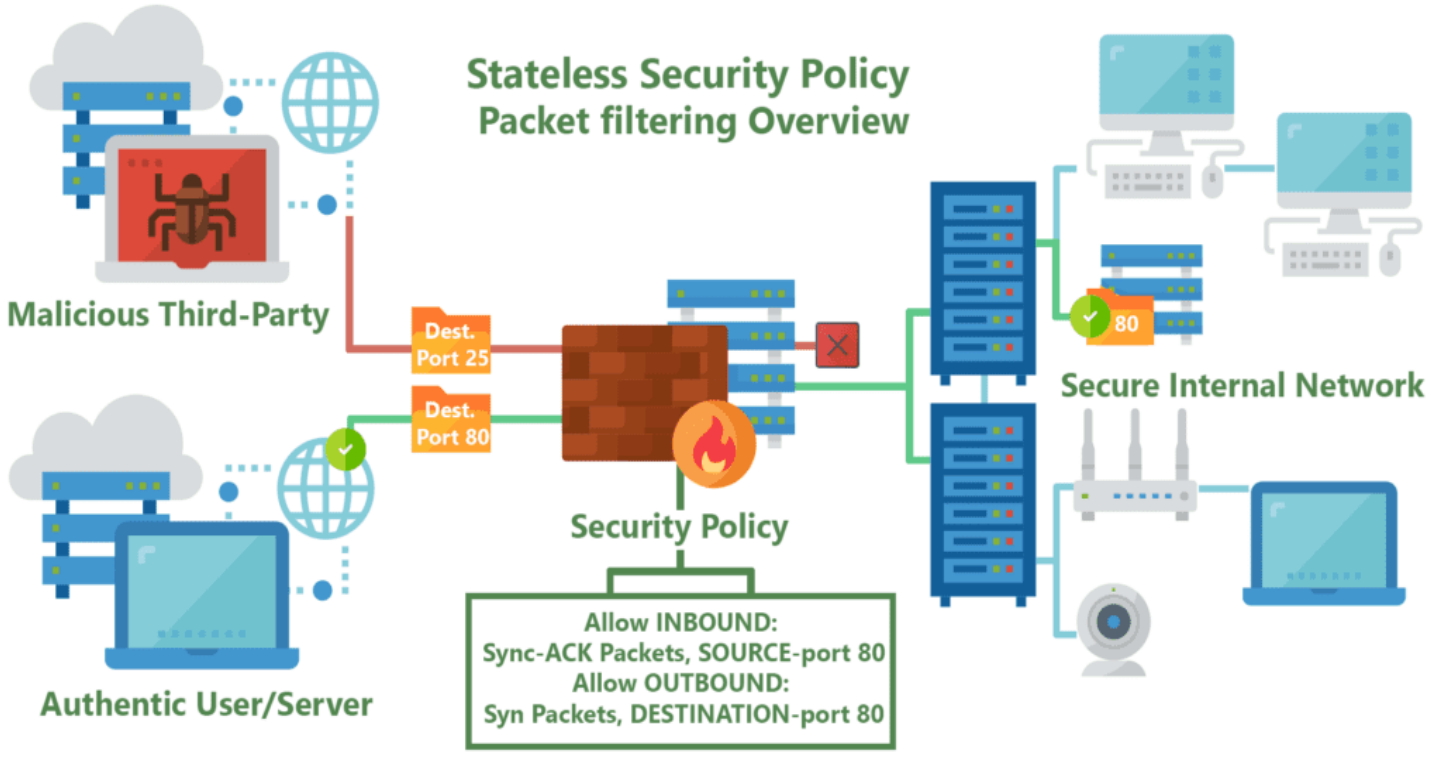
Principes de la sauvegarde :

- Sauvegarde **totale** : toutes les informations sont sauvegardées
- Sauvegarde **différentielle** : seules les informations modifiées depuis la dernière sauvegarde complète sont sauvegardées
- Sauvegarde **incrémentielle** : seules les informations modifiées depuis une sauvegarde totale ou incrémentielle



4) Sécuriser le réseau

Les cyberattaques (ransomwares, malwares, phishing et autres virus) sont des agressions extérieures qu'il faut pouvoir bloquer avec un **pare-feu** et un **proxy** qui protègent les connexions web. La cybersécurité d'une entreprise passe aussi par la protection du réseau local, des accès wifi, de la messagerie électronique ainsi que de tout accès distant : https://owasp.org/www-project-top-ten/#div-translation_efforts.



5) Protéger les terminaux mobiles

- Ordinateurs **portables / tablettes** : Avec un antivirus adapté et mis à jour

  Exemple de source d'informations :

  https://www.av-comparatives.org/

- **Smartphone**s : Il existe aujourd'hui des antivirus et des anti-malwares pour mobiles. Cependant, une controverse existe sur l'utilité d'un tel logiciel sur ce support… Une simple recherche sur Internet, en montre les limites.

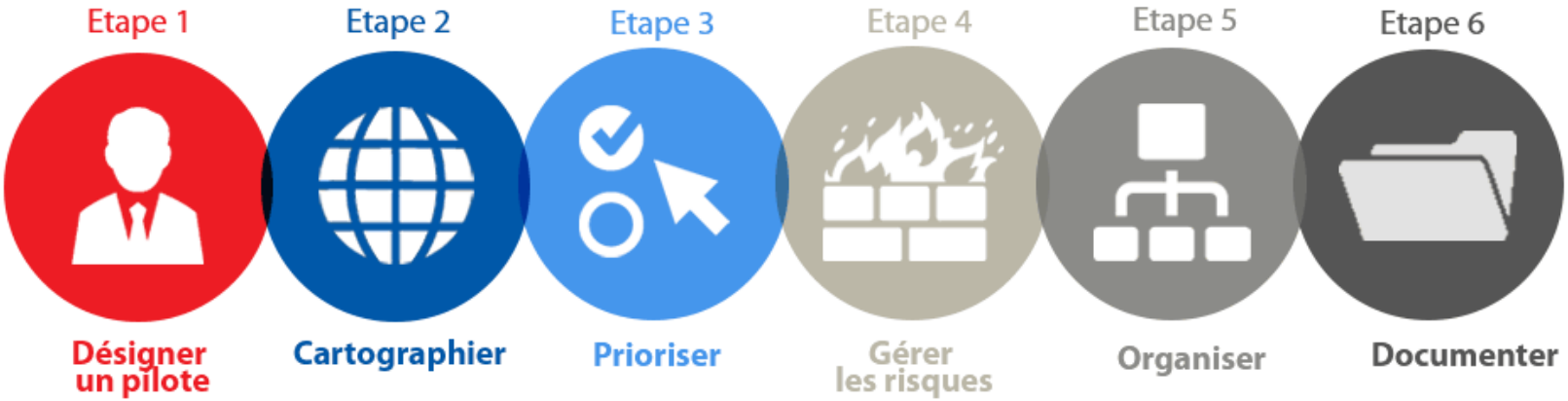
  https://www.01net.com/actualites/pour-securiser-android-google-est-force-de-faire-la-police-dans-son-ecosysteme-1665793.html

Il faut également penser à activer le verrouillage automatique pour empêcher toute utilisation frauduleuse en cas de perte/vol.

6) Protéger les données personnelles

Le nouveau **Règlement Européen de Protection des Données Personnelles** (RGPD) exige la mise en place d'une politique de protection de la vie privée.

Il faut donc intégrer une clause de confidentialité dans les contrats de sous-traitance informatique avec les prestataires informatiques et fournisseurs Cloud (surtout depuis le vote du Cloud Act).



7) Gérer les données sensibles

Les fichiers confidentiels d'une entreprise doivent à minima être :

- **Encryptés** lors de leur sauvegarde (le chiffrement des données considérées comme sensibles au regard de la loi est obligatoire)
- **A accès limité** aux personnes habilitées (connexion grâce à une authentification personnelle).

→ Méthode de cryptage symétrique : chiffrement et déchiffrement à l'aide de la même clé (DES, AES)

→ Méthode de cryptage asymétrique : utilisation d'une clé privée et d'une clé publique via un serveur (RSA)

Dans ce dernier cas, se pose le problème de l'authentification des utilisateurs.

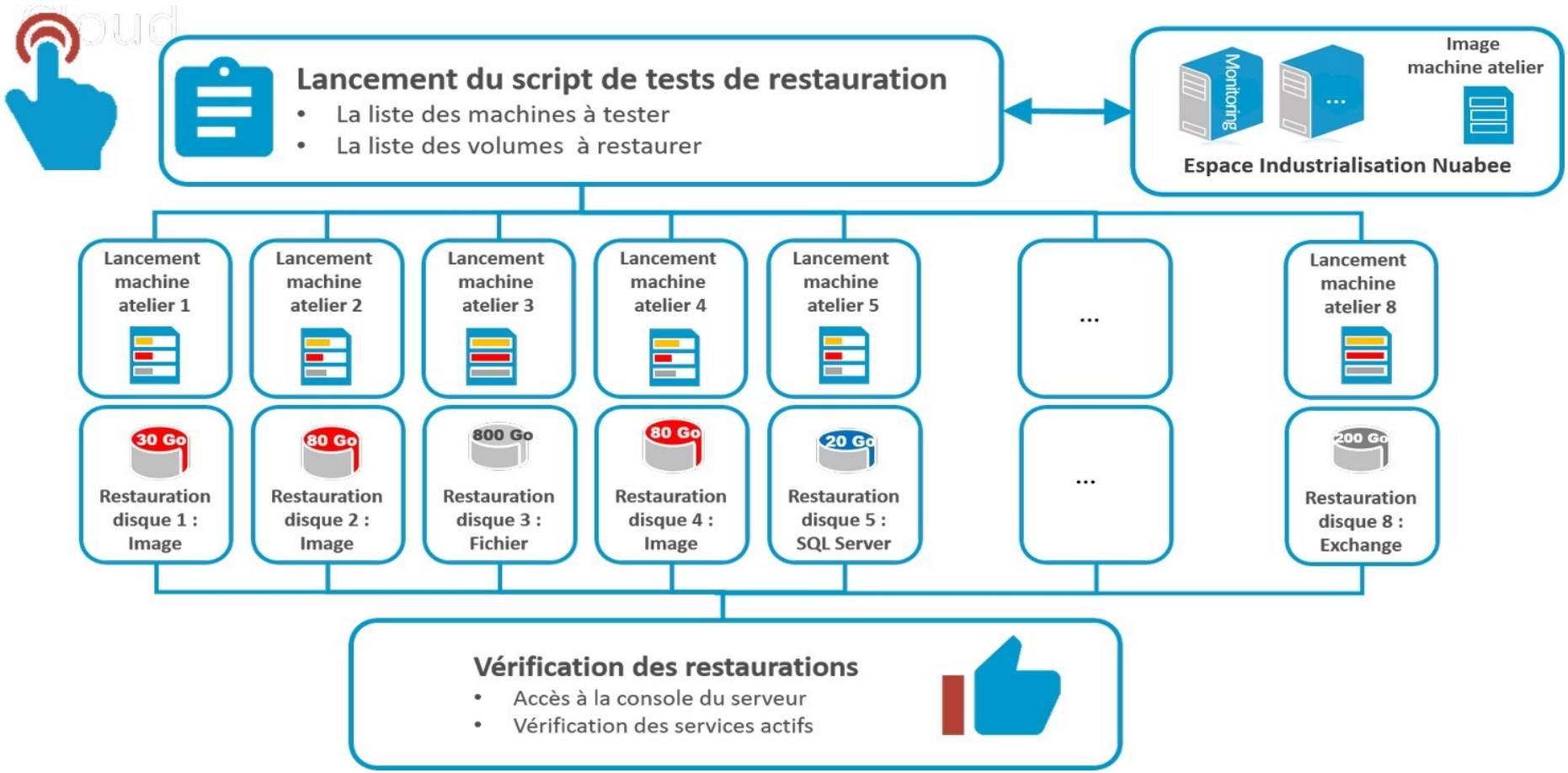
8) Sécuriser les locaux

Les locaux d’une entreprise restent son point névralgique.

L'accès physique des bureaux et serveurs informatiques doit absolument être sécurisé : accès fermé et contrôlé avec digicodes et autres badges nominatifs pour les personnes habilitées.

9) Faire des tests de sécurité

Tout comme les exercices d'évacuation, les **tests de restauration des données** (fichiers, images système, serveurs et systèmes d'exploitation) sont nécessaires pour se préparer aux prochaines cyberattaques.



10) Assurer la continuité en cas d'attaque

Si malgré toutes ces mesures l'entreprise est victime d'une cyberattaque, il est possible de reprendre son activité dans encombres et sans payer de rançon. La solution ? L'anticipation !

Mettre en place un **Plan de Reprise d'Activité** grâce à un logiciel de sauvegarde spécialisé permet de restaurer toutes les données perdues ou encryptées en quelques heures !

	Espace de stockage gratuit	Prix/mois	Taille de fichiers	Compatibilité	Historique des fichiers	Option de sauvegarde	Chiffrement stockage/transferts	Pays
Dropbox	2 Go (extensible à 20 Go par parrainages et astuces)	8,25 $/1 To 12,50 $/2 To 20 $/Illimité	Illimité (10 Go via interface Web)	Windows, macOS, Linux, Android, iOS, Kindle Fire, Windows Phone	30 jours	Non	Oui	USA
Box	10 Go	8 €/100 Go	250 Mo (gratuite) 5 Go (payante)	Windows, macOS, Android, iOS	Oui (compte payant uniquement)	Non	Oui	USA
Google Drive	15 Go	1,99 €/100 Go 9,99 €/1 To 99,99 $/10 To	5 To	Windows, macOS, Android, iOS	30 jours	Oui	Oui	USA
Microsoft OneDrive	5 Go	2 €/50 Go 7 €/1 To (+ Office 365) 10 €/5 To (+ Office 365 pour 5 utilisateurs)	15 Go	Windows, macOS, Android, iOS, Windows Phone	25 versions précédentes	Non	Transferts uniquement	USA
Amazon Cloud Drive	5 Go	1 $/100 Go 5$/1 To	Illimitée	Windows, macOS, Android, iOS	Non	Non	Transferts uniquement	USA
Apple ICloud	5 Go	0,99 €/50 Go 2,99 €/200 Go 9,99 €/2 To	Illimitée	Windows, macOS, iOS	Non	Terminaux iOS uniquement	Oui	USA
HubiC	25 Go	1 €/100 Go 5 €/10 To	Illimitée	Windows, macOS, Linux, Android, iOS, Windows Phone 8	Versions précédentes (illimité)	Oui	Oui	France