# Sensibilisation Cybersécurité

## Comment protéger ma TPE-PME ?

# Pourquoi sécuriser mon SI ?

# Pourquoi sécuriser mon SI ?

**1**

## Les risques cybersécurité sont systémiques

- 10 minutes pour recevoir la première attaque en Nouvelle-Calédonie
- Plusieurs cas de CryptoLocker en Nouvelle-Calédonie

**2**

## La cybercriminalité est en hausse spectaculaire :

- 80 % des entreprises françaises ont constaté au moins une cyberattaque dans l'année*
- 60% des PME victimes disparaissent au cours des six mois*

**3**

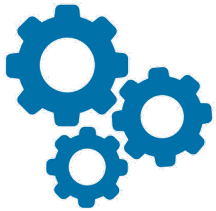
## Les contraintes règlementaires sont en constante évolution

- RGPD, directive NIS, LPM **
- Exigences contractuelles

* Baromètre annuel du CESIN publié en janvier 2019 & Etude Accenture 2019
** RGPD : Règlement général sur la protection des données
** NIS : Network and Information System Security
** LPM : Loi de Programmation Militaire

cci NOUVELLE-CALÉDONIE

# Quels peuvent être les impacts ?



Ralentissement/arrêt de la production


Indisponibilité du site web

Perte/altération des données

Fuite des données

# Comment sécuriser mon SI ?

# Avant de commencer

# Par où commencer ?

| | |
|---|---|
| 1- Choisir un référentiel | • Choisir un guide public adapté à ma structure<br>• Se concentrer sur les risques cyber les plus répandus<br>• Se concentrer sur les règles les plus critiques (80/20) |
| 2- Identifier les systèmes critiques | • Prioriser les chantiers (par où commencer ?)<br>• Définir un schéma directeur à long terme (Ex : 3 ans) |
| 3- Choisir l'équipe technique | • Equipe interne si possible<br>• Equipe externe (prestataire de service informatique) |
| 4- Choisir un chef d'orchestre | • Suivi des prestataires ou des équipes internes<br>• Reporting à la direction |

# Combien ça coûte ?

# Le coût de la cybersécurité

## Coût d'investissement initial

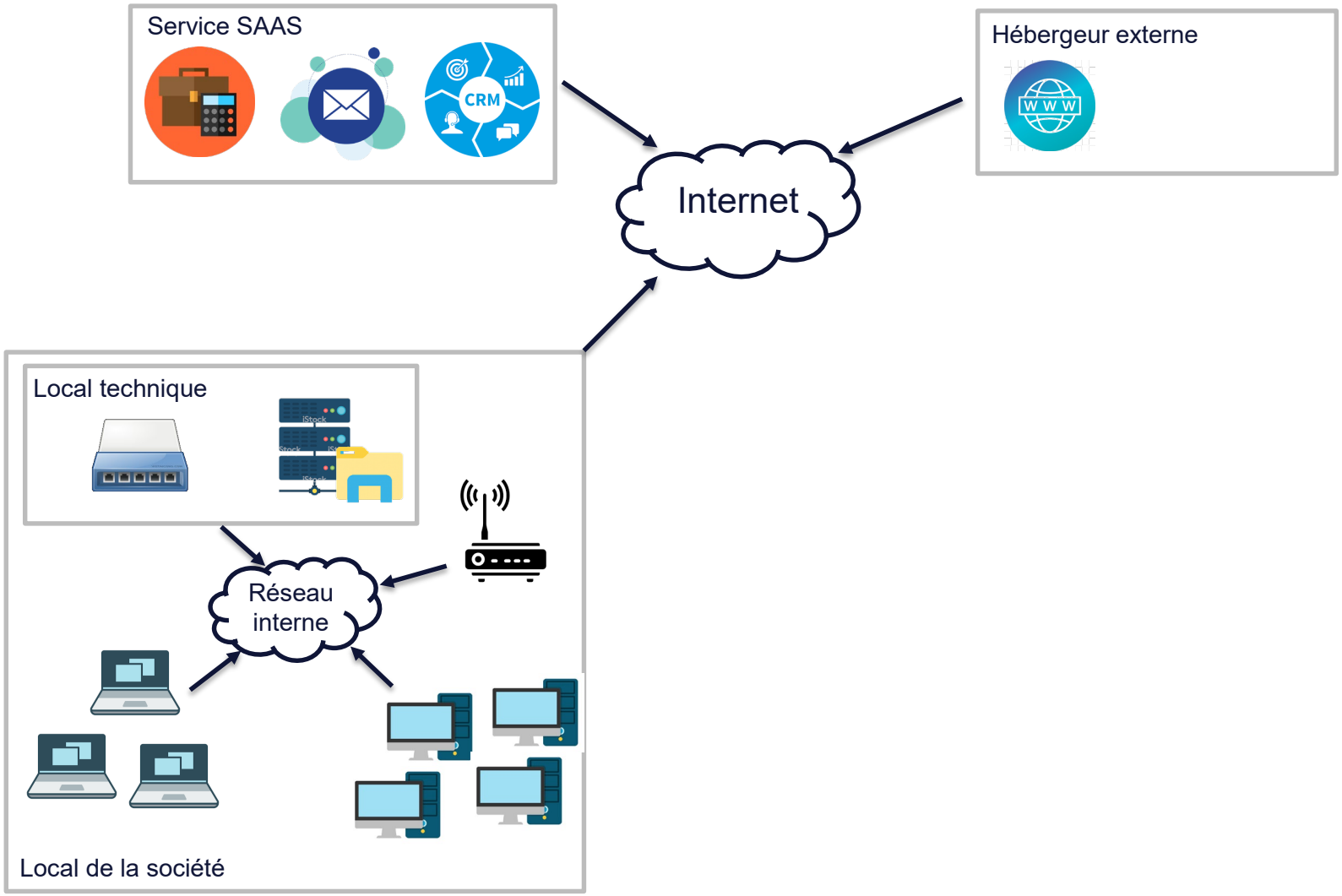
Dépend de :
- Niveau de sécurité actuel
- Taille du système
- Contexte de l'entreprise
- Réglementation applicable
- Engagement contractuel

## Maintien en condition de sécurité

Estimé à 10 % du coût total de l'informatique

# Exemple concret

# La société


Service SAAS
CRM
Hébergeur externe
WWW
Internet
Local technique
Réseau
interne
Local de la société

# Etape 1 : Choix du référentiel

**1- Choisir un référentiel**

- Choisir un guide public adapté à ma structure
- Se concentrer sur les risques cyber les plus répandus
- Se concentrer sur les règles les plus critiques (80/20)

**2- Identifier les systèmes critiques**

- Prioriser les chantiers (par où commencer ?)
- Définir un schéma directeur à long terme (Ex : 3 ans)

**3- Choisir l'équipe technique**

- Equipe interne
- Equipe externe (prestataire de service informatique)

**4- Choisir un chef d'orchestre**

- Suivi des prestataires
- Reporting à la direction

# Les sources publiques disponibles

https://www.ssi.gouv.fr/
https://www.cert.ssi.gouv.fr/

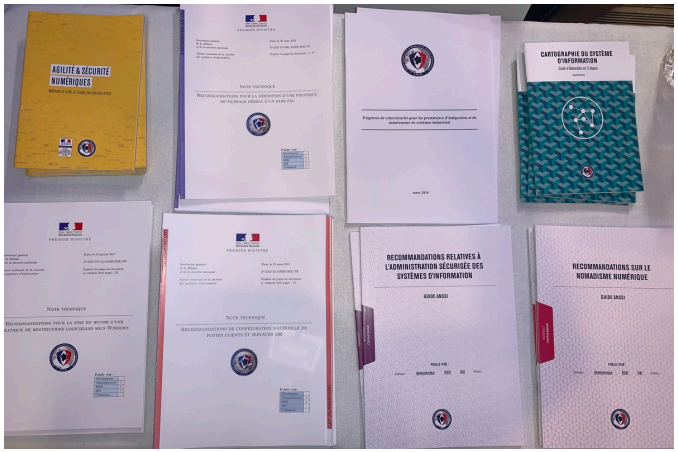
https://www.cnil.fr/fr/cybersecurite

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

https://sisse.entreprises.gouv.fr/fr
Service de l'Information Stratégique
et de Sécurité Economique

# Les guides publics disponibles






# Les guides publics disponibles


**Fraicheur navigateur : A**

FAQ Tester à nouveau

**Sécurisation courriels : D**

FAQ Informations détaillées

**Sauvegardes données : B**

FAQ

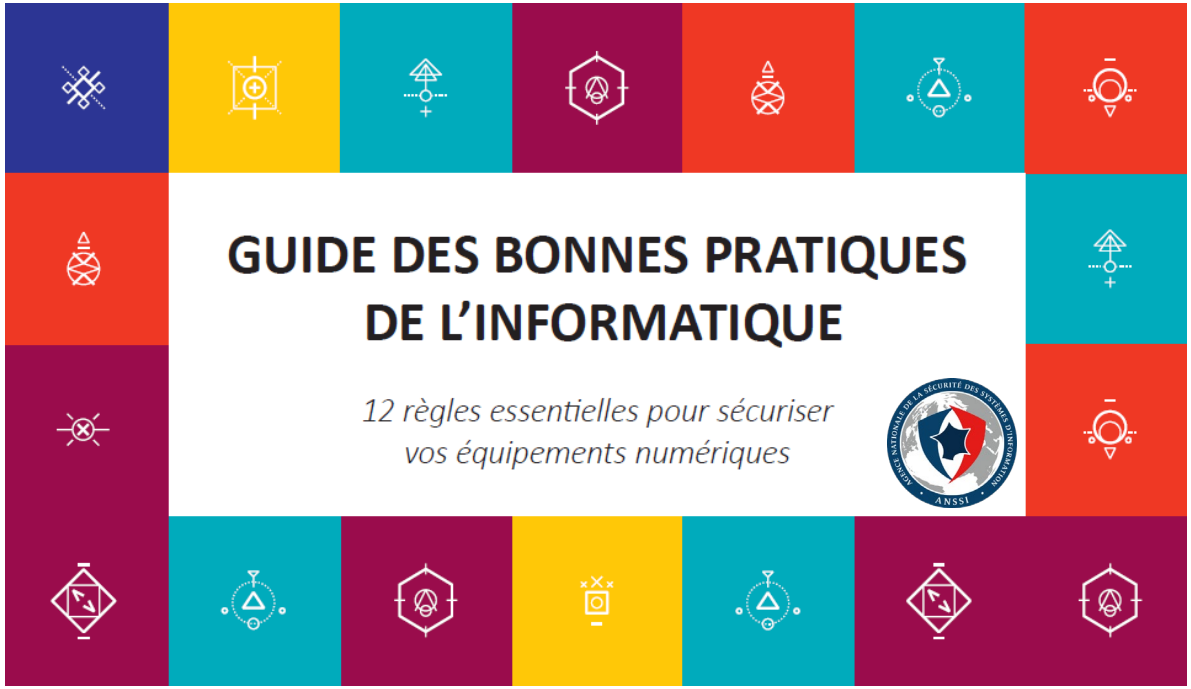
**Solidité mot de passe : A**

FAQ

https://ssi.economie.gouv.fr/

# Le guide le plus adapté :

*Guide de l'ANSSI pour petites et moyennes entreprises*




Next…
Identification des règles prioritaires sous forme de projet

# Projet 1 : Gestion de la sauvegarde


## Effectuer des sauvegardes régulières

# Projet 1 : Gestion de la sauvegarde

## 1. Sauvegarder régulièrement les données sensibles sur un support externe

## 2. Externaliser la sauvegarde

- Intégrer les clauses et exigences de sécurité (Cf. *Guide d'externalisation de l'ANSSI*)
- Intégrer les clauses liées au RGPD
- Exiger une sauvegarde offline des données

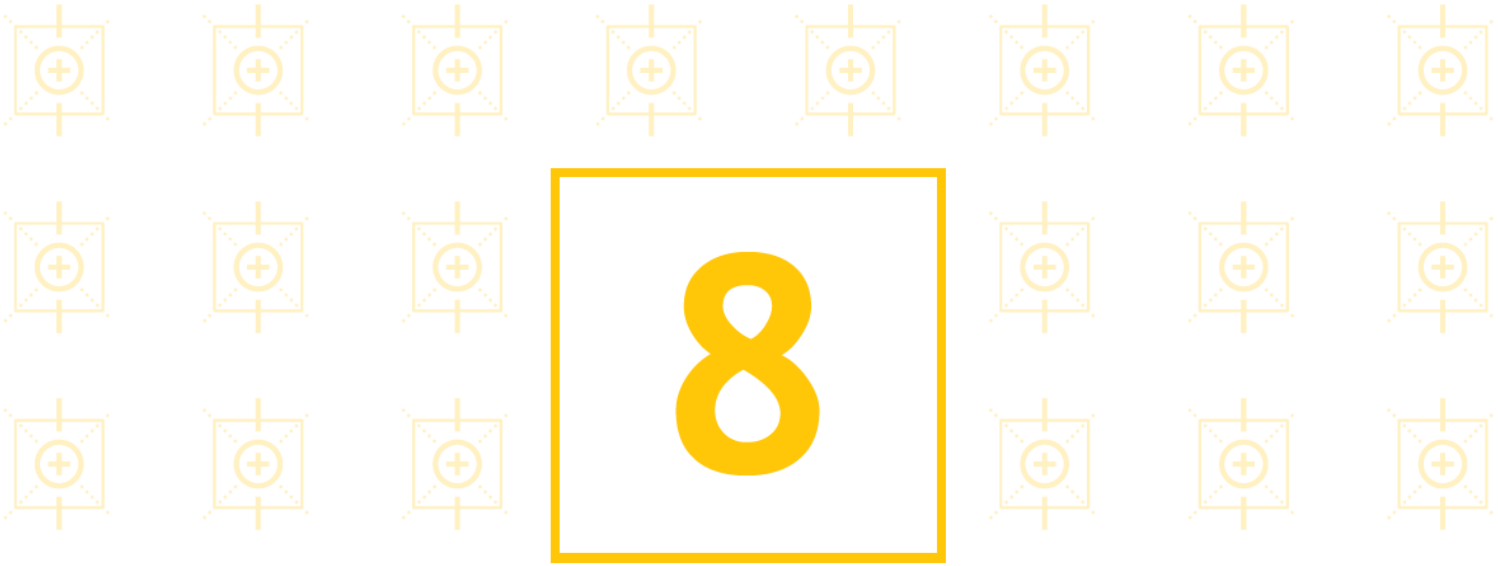
## 3. Imposer contractuellement la sauvegarde aux fournisseurs de service

- Service SAAS, Hébergement du site web, etc.

## 4. Tester la sauvegarde

- Formaliser la procédure de restauration des données
- Effectuer un test une fois par an.

# Projet 2 : Sécuriser la messagerie




## Être prudent lors de l'utilisation de sa messagerie

# Projet 2 : Sécuriser la messagerie

## 1. Déployer et configurer un anti-spam

- Au niveau du serveur de messagerie
- Au niveau du client de messagerie

## 2. Déployer et configurer un anti-malware

- Au niveau du serveur de messagerie
- Au niveau des postes de travail

## 3.Déployer et configurer un Pare-feu public et activer le module anti-phishing

## 4. Déployer et configurer une protection anti-phishing :

- Blocage en fonction de la réputation de l'adresse IP, du nom de domaine ou de l'@ émetteur
- Blocage en cas d'échec d'authentification de l'émetteur (SPF, DKIM et DMARC)
- Blocage en fonction des pièces jointes

## 5. Durcir la configuration de ma solution de messagerie

- Activer les paramètres de sécurité

# Projet 3 : Installer les mises à jour


## Mettre à jour régulièrement vos logiciels

# Projet 3 : Installer les mises à jour

1. **Upgrader les systèmes d'exploitation (Windows 7, Windows Server 2003, etc.)**
2. **Supprimer tout ce qui n'est pas nécessaire (PC et Serveur)**
3. **Configurer une installation automatique des mises à jour de sécurité sur les PC**
   - Système d'exploitation (Windows, Linux, etc.)
   - Logiciel utilisé (Adobe, Flash, Chrome, etc.)
4. **Pour les équipements d'infrastructure, prévoir un déploiement périodique :**
   - Serveur, Routeur, Switch, NAS, Baie SAN, etc.
   - Nous recommandons une période de 2 à 6 mois, sauf mise à jour critique.
5. **Pour les équipements sensibles, prévoir un déploiement dans les meilleurs délais :**
   - Serveur exposé, Service/application exposé, Pare-feu public, etc.
   - Nous recommandons un délais de 3 à 5 jours.
6. **Pour les applications métiers, demander à l'éditeur de mettre à jour les composants :**
   - Serveur d'application, CMS, PHP, Java, MySQL, etc.
7. **Pour les applications hébergées en externe, imposer contractuellement les MAJ :**
   - Composants techniques de mon site web
   - Composants techniques de mes services SAAS (messagerie, CRM, logiciel de comptabilité, etc.)

# Projet 3 : Installer les mises à jour

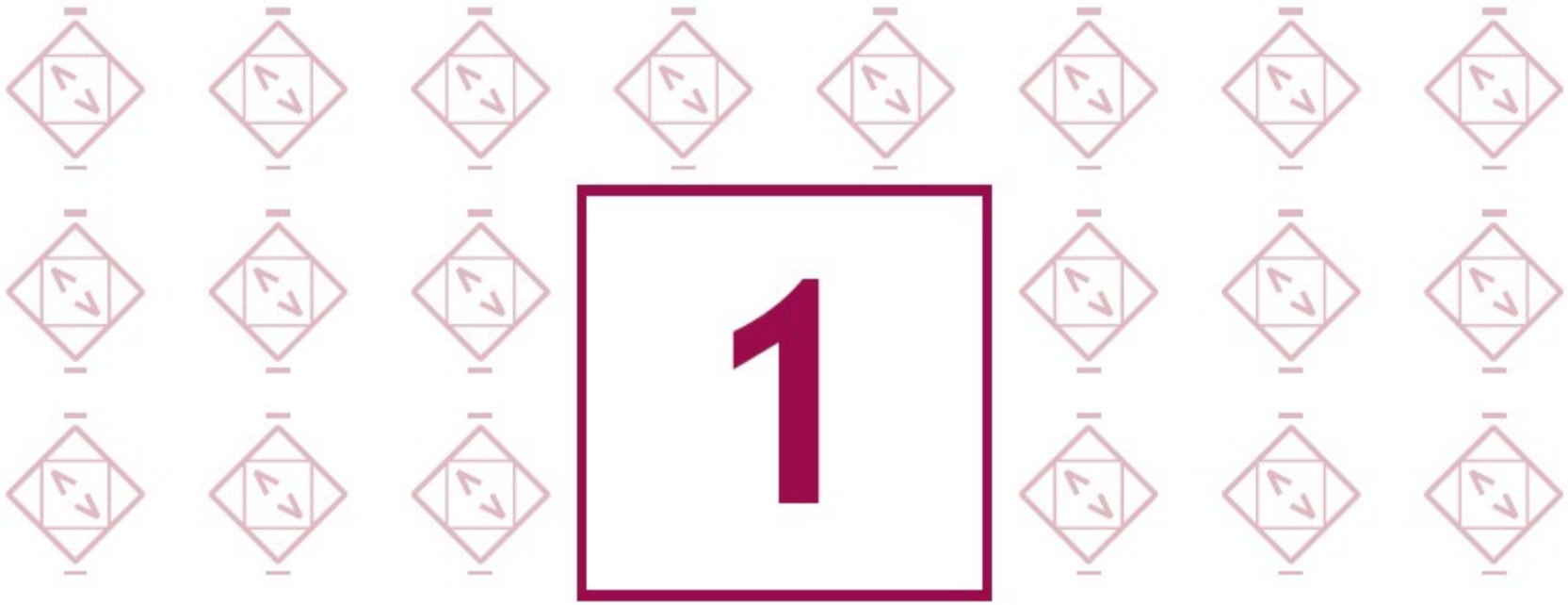
## Exemple de clause pour les mises à jour :

***Mise à jour initiale :***
Tous les composants et services constituant l'application ou le système doivent être dans une dernière version intégrant l'ensemble des mises à jour de sécurité.

***Mise à jour périodique :***
Le prestataire s'engage à appliquer périodiquement les correctifs de sécurité sur tous les matériels et logiciels dont il a la charge après les avoir validés, à minima une fois par mois.

***Veille sur les mises à jour critiques :***
Le prestataire doit déployer un processus de veille sur les menaces et vulnérabilités sur les produits et technologies mises en œuvre sur les systèmes qu'il a déployés. Il pourra s'appuyer sur les informations publiées par les CERT étatiques ou privés ainsi que les sites web des éditeurs.
En cas de vulnérabilité critique le prestataire doit installer les mises à jour dans un délais de 4 jours. En cas de contrainte, le prestataire doit réduire les risques d'exploitation de cette vulnérabilité en appliquant des mesures compensatoires.

# Projet 4 : Gestion des mots de passe




## Choisir avec soin ses mots de passe

# Projet 4 : Gestion des mots de passe

## Définir et appliquer une politique de mot de passe

### Formaliser la politique

Exemple :

- Minimum 12 caractères
- Un mot de passe par application
- Pas de réutilisation
- Blocage pendant 1h en cas de 10 tentatives

### Informer les utilisateurs

- Envoyer un e-mail
- Changer les mots de passe sur toutes les applications (internes ou externes)
- Utiliser la solution KeePass (demander à un salarié de faire un guide)

### Informer les prestataires

- Envoyer un e-mail
- Appliquer la nouvelle politique de mot de passe sur le périmètre de chaque prestataire
- Demander une preuve d'application de la politique

# Projet 5 : Gestion des comptes

3

## Bien connaître ses utilisateurs et ses prestataires

# Projet 5 : Gestion des comptes

## 1. Utiliser des comptes utilisateurs qui ne disposent pas de privilège d'administration

## 2. Sur chaque application/service, faire une revue des comptes et des droits

- Supprimer les comptes fantômes
- Supprimer les droits d'accès non nécessaire
- Supprimer les comptes génériques (admin, stagiaire, etc.) et les remplacer par des comptes nominatifs

## 3. Rédiger et appliquer une politique d'arrivée et de départ :

- Attribuer uniquement les droits nécessaires pour accomplir les missions. Tracer les accès dans un fichier.
- En cas de départ d'un salarié, supprimer/désactiver son compte sur toutes les applications/systèmes
- En cas de changement de fonction d'un salarié, modifier ses droits d'accès.
- En cas de longue absence, désactiver les droits.

## 4.Maîtriser l'accès des prestataires :

- Accès nominatif et ouverture à la demande.

# Ainsi de suite ….

6 7 …. 12

+

A Sensibiliser l'ensemble des salariés

B Intégrer la sécurité dans les projets

C Tester mon site web

D Tester ma messagerie

# A

## Sensibiliser l'ensemble des salariés


https://www.hack-academy.fr/


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


https://www.youtube.com/


https://www.cybersecuritycoalition.be/resource/cyber-security-kit-french/


https://secnumacademie.gouv.fr/


https://phishingquiz.withgoogle.com/

# B

## Intégrer la sécurité dans les projets

**Intégrer la sécurité en amont des projets**
**« Security By Design »**

# B Intégrer la sécurité dans les projets

**Exigence à respecter par le prestataire**

**Clause de sécurité pour la prestation**

**Exigence à respecter par l'application**

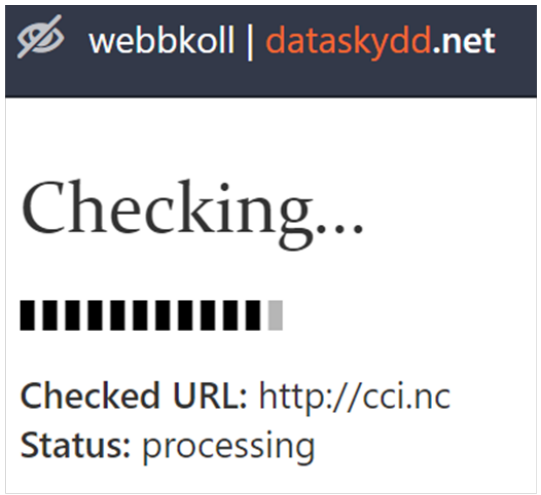


**Clauses de sous-traitance**

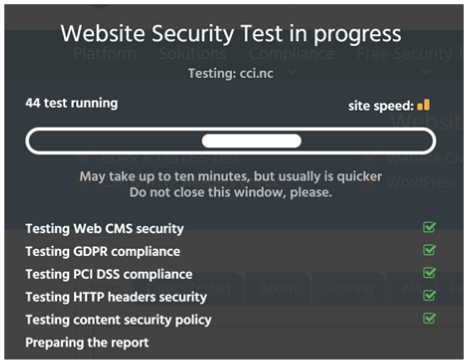
CNIL.

# C

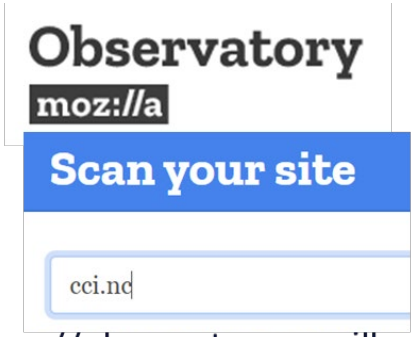
## Tester la sécurité de mon site web




https://webbkoll.dataskydd.net/en/


https://www.immuniweb.com/websec/

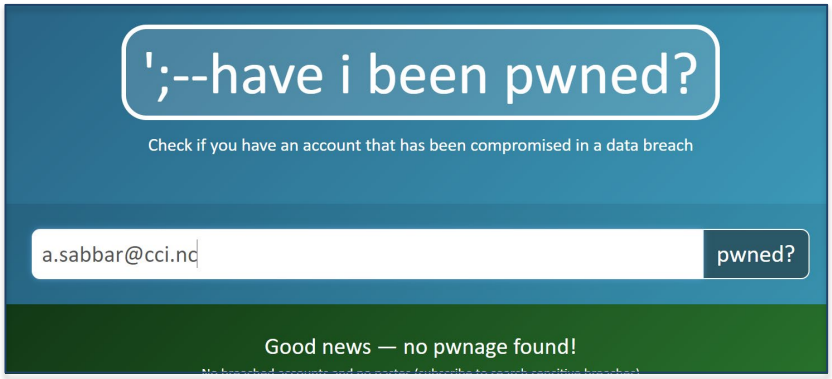



https://observatory.mozilla.org/


https://www.cookiebot.com/fr/

# D

## Tester la sécurité de ma messagerie




https://haveibeenpwned.com/


https://mxtoolbox.com/


https://gcatoolkit.org/smallbusiness/


https://dmarcguide.globalcyberalliance.org

# Etape 2 : Identifier les systèmes critiques

| | |
|---|---|
| 1- Choisir un référentiel | • Choisir un guide public adapté à ma structure<br>• Se concentrer sur les risques cyber les plus répandus<br>• Se concentrer sur les règles les plus critiques (80/20) |
| **2- Identifier les systèmes critiques** | • Prioriser les chantiers (par où commencer ?)<br>• Définir un schéma directeur à long terme (Ex : 3 ans) |
| 3- Choisir l'équipe technique | • Equipe interne<br>• Equipe externe (prestataire de service informatique) |
| 4- Choisir un chef d'orchestre | • Suivi des prestataires<br>• Reporting à la direction |

# Classification des systèmes

## 1- Quels sont les impacts en cas :

- ✓ D'indisponibilité du système
- ✓ De perte des données du système
- ✓ De compromission des données

## 2- Classifier les systèmes en fonction de la gravité des impacts :

- ✓ Impact financier (perte du CA, sanction, rançon)
- ✓ Impact sur l'image
- ✓ Impact juridique
- ✓ Etc.

# Classification des systèmes

## Site web — 1/3

- Absence de visibilité sur internet
- Impact sur l'image suite à une défiguration

## Messagerie — 3/3

- Fuite des données confidentielles
- Impact sur les opérations (indisponibilité)
- Vecteur d'intrusion pour mes clients

## CRM — 3/3

- Perte des données clients
- Fuite des données clients (contacts, prestations, etc.)
- Impact sur les opérations (indisponibilité)

## Comptabilité — 2/3

- Perte des données financières
- Fuite des données financières

## Partage réseau — 2/3

- Perte des données projets et du savoir-faire
- Fuite de mon savoir-faire
- Impact sur les opérations (indisponibilité)

1/3 Non critique

2/3 Important

3/3 Critique

# Classification des systèmes

| | |
|---|---|
| Critique | • Messagerie<br>• CRM |
| Important | • Logiciel de comptabilité<br>• Répertoire interne |
| Non critique | • Site internet |

Les projets seront appliqués, en priorité, sur les systèmes critiques

# Etape 3 : Choisir l'équipe

| | |
|---|---|
| 1- Choisir un référentiel | • Choisir un guide public adapté à ma structure<br>• Se concentrer sur les risques cyber les plus répandus<br>• Se concentrer sur les règles les plus critiques (80/20) |
| 2- Identifier les systèmes critiques | • Prioriser les chantiers (par où commencer ?)<br>• Définir un schéma directeur à long terme (Ex : 3 ans) |
| **3- Choisir l'équipe technique** | • Equipe interne<br>• Equipe externe (prestataire de service informatique) |
| 4- Choisir un chef d'orchestre | • Suivi des prestataires<br>• Reporting à la direction |

# Choix de l’équipe


Editeurs/fournisseurs
de mes applications

Des prestataires de service
informatique

# Etape 4 : Choisir un chef d'orchestre

| | |
|---|---|
| 1- Choisir un référentiel | • Choisir un guide public adapté à ma structure<br>• Se concentrer sur les risques cyber les plus répandus<br>• Se concentrer sur les règles les plus critiques (80/20) |
| 2- Identifier les systèmes critiques | • Prioriser les chantiers (par où commencer ?)<br>• Définir un schéma directeur à long terme (Ex : 3 ans) |
| 3- Choisir l'équipe technique | • Equipe interne<br>• Equipe externe (prestataire de service informatique) |
| **4- Choisir un chef d'orchestre** | • Suivi des prestataires<br>• Reporting à la direction |

# Choix du chef d’orchestre

Motivé

Connaissance IT

Disponible

Organisé

# Pour toute question

Contactez-moi : rssi@cci.nc