LOCKSELF

Checklist : 42 mesures pour protéger le SI

Télécharger cette checklist

Sensibiliser et former

- **Former les équipes opérationnelles** à la sécurité des systèmes d'information.
- **Sensibiliser les utilisateurs** aux bonnes pratiques élémentaires de sécurité informatique.
  - ***Mesure renforcée :*** *élaboration et signature d'une charte des moyens informatiques.*
- **Maîtriser les risques** de l'infogérance.

Connaître le système d'information

- **Identifier les informations et serveurs** les plus sensibles et maintenir un schéma du réseau.
- **Disposer d'un inventaire exhaustif** des comptes privilégiés et le maintenir à jour.
- **Organiser les procédures d'arrivée, de départ et de changement** de fonction des utilisateurs.
  - ***Mesure renforcée :*** *formalisation et mises à jour des procédures en fonction du contexte.*
- **Autoriser la connexion au réseau de l'entité** aux seuls équipements maîtrisés.
  - ***Mesure renforcée :*** *compléter les aménagements par des mesures techniques telles que l'authentification des postes sur le réseau.*

Authentifier et contrôler les accès

- **Identifier** nommément **chaque personne** accédant au système **et distinguer les rôles utilisateur / administrateur.**
  - ***Mesure renforcée :*** *Activation de la journalisation liée aux comptes.*
- **Attribuer les bons droits** sur les ressources sensibles du système d'information.
- **Définir et vérifier des règles de choix et de dimensionnement** des mots de passe.

LOCKSELF

Checklist : 42 mesures pour protéger le SI

- ◯ **Protéger les mots de passe** stockés sur les systèmes.
- ◯ **Changer les éléments d'authentification par défaut** sur les équipements et services.
  - ◯ ***Mesure renforcée :*** *Après le changement, renouveler régulièrement.*
- ◯ **Privilégier** lorsque c'est possible **une authentification forte.**
  - ◯ ***Mesure renforcée :*** *Privilégier les cartes à puces ou, à défaut, les mécanismes de mots de passe à usage unique (ou One TIme Password) avec jeton physique.*

Sécuriser les postes

- ◯ **Mettre en place un niveau de sécurité minimal** sur l'ensemble du parc informatique.
  - ◯ ***Mesure renforcée :*** *Effectuer et tester régulièrement des sauvegardes déconnectées des données vitales, les stocker sur des équipements déconnectés et vérifier périodiquement leur restauration.*
- ◯ **Se protéger des menaces relatives** à l'utilisation de supports amovibles.
  - ◯ ***Mesure renforcée :*** *Utiliser des solutions permettant d'interdire l'excécution de programmes sur les périphériques amovibles et implémenter une procédure de mise au rebut stricte.*
- ◯ **Utiliser un outil de gestion centralisée** afin d'homogénéiser les politiques de sécurité.
- ◯ **Activer et configurer le pare-feu local** des postes de travail.
  - ◯ ***Mesure renforcée :*** *Configurer le pare-feu pour bloquer par défaut tous les flux, notamment les ports d'administration, n'autoriser que les services nécessaires depuis des équipements identifiés, et journaliser les flux bloqués.*
- ◯ **Chiffrer les données sensibles** transmises par voie Internet.

Sécuriser le réseau

- ◯ **Segmenter le réseau et mettre en place un cloisonnement** entre ces zones.
- ◯ **S'assurer de la sécurité des réseaux** d'accès Wi-Fi et de **la séparation des usages.**
- ◯ **Utiliser des protocoles réseaux sécurisés** dès qu'ils existent.

LOCKSELF

Checklist : 42 mesures pour protéger le SI

- ◯ **Mettre en place une passerelle d'accès sécurisé** à Internet.
  - ◯ ***Mesure renforcée :*** *Mettre en place des mécanismes de sécurité sur le serveur mandataire, maintenir les équipements en sécurité, prévoir leur redondance, désactiver les résolutions DNS directes sur les terminaux, et établir une connexion sécurisée pour les postes nomades.*
- ◯ **Cloisonner les services visibles** depuis Internet du reste du système d'information.
- ◯ **Protéger sa messagerie professionnelle.**
  - ◯ ***Mesure renforcée :*** *Mettre en place un serveur relais dédié pour l'envoi et la réception des messages, déployer un service anti-spam efficace, et configurer correctement les mécanismes d'authentification et les enregistrements DNS publics (MX, SPF, DKIM, DMARC) pour sécuriser l'infrastructure de messagerie.*
- ◯ **Sécuriser les interconnexions réseau** dédiées avec les partenaires.
  - ◯ ***Mesure renforcée :*** *Dédier un équipement de filtrage IP pour les connexions partenaires, envisager l'ajout d'un système de détection d'intrusions, et maintenir à jour un point de contact chez le partenaire pour une réaction rapide en cas d'incident de sécurité.*
- ◯ **Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques.**

Sécuriser l'administration

- ◯ **Interdire l'accès à Internet depuis les postes ou serveurs utilisés** pour l'administration du système d'information.
  - ◯ ***Mesure renforcée :*** *Récupérer les mises à jour logicielles depuis une source sûre, les contrôler, les transférer sur un poste d'administration isolé d'Internet via un support amovible dédié, et envisager une zone d'échanges pour automatiser certaines tâches.*
- ◯ **Utiliser un réseau dédié et cloisonné** pour l'administration du système d'information.
  - ◯ ***Mesure renforcée :*** *Privilégier un cloisonnement physique des réseaux lorsque cela est possible.*
- ◯ **Limiter au strict besoin opérationnel les droits d'administration** sur les postes de travail.

LOCKSELF

Checklist : 42 mesures pour protéger le SI

Gérer le nomadisme

- ◯ **Prendre des mesures de sécurisation physique des terminaux nomades.**
  - ◯ ***Mesure renforcée :*** *Envisager l'utilisation d'un support externe (carte à puce ou jeton USB) pour stocker les secrets de déchiffrement ou d'authentification, et le conserver séparément du poste pour renforcer la sécurité.*
- ◯ **Chiffrer les données sensibles,** en particulier sur le matériel potentiellement perdable.
- ◯ **Sécuriser la connexion réseau des postes utilisés en situation de nomadisme.**
  - ◯ ***Mesure renforcée :*** *Mettre en place une authentification forte, combinant un mot de passe avec un certificat sur support externe ou un mécanisme de mot de passe à usage unique, pour prévenir la réutilisation d'authentifiants en cas de vol ou de perte du poste.*
- ◯ **Adopter des politiques de sécurité dédiées aux terminaux mobiles.**
  - ◯ ***Mesure renforcée :*** *Opter pour des terminaux mobiles sans assistant vocal intégré. Ceci augmente sensiblement la surface d'attaque du terminal.*

Maintenir le système d'information à jour

- ◯ **Définir une politique de mise à jour des composants du système d'information.**
- ◯ **Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles.**

Superviser, auditer, réagir

- ◯ **Activer et configurer les journaux** des composants les plus importants.
  - ◯ ***Mesure renforcée :*** *Centraliser les journaux sur un dispositif dédié pour faciliter la recherche d'événements suspects, archiver les journaux sur le long terme, et empêcher un attaquant d'effacer ses traces sur les équipements compromis.*
- ◯ **Définir et appliquer une politique de sauvegarde** des composants critiques.
  - ◯ ***Mesure renforcée :*** *Planifier au moins une fois par an un exercice de restauration des données et conserver une trace technique des résultats.*

LOCKSELF

Checklist : 42 mesures pour protéger le SI

- [ ] **Procéder aux contrôles et audits de sécurité réguliers** puis **appliquer** les actions correctives associées.
- [ ] **Désigner un référent en sécurité des systèmes d'information** et le faire connaître auprès du personnel.
- [ ] **Définir une procédure de gestion des incidents de sécurité.**

Pour aller plus loin

- [ ] **Renforcée : Mener une analyse de risques formelle**
- [ ] **Renforcée : Privilégier l'usage de produits et de services qualifiés par l'ANSSI.**