CERT Santé

Mesures « quick-win » pour renforcer la résilience de son SI en vue des JOP

21/03/2024

FSSI / CERT-FR / CERT Santé

Intervenants

Patrice Bigeard (FSSI)

Prachea THIOUNN (CERT-FR)

Florent FAUVIN (CERT-FR)

Quentin LE THIEC (CERT Santé)

Thomas DAMONNEVILLE (CERT Santé)

CERT Santé

Introduction

Patrice Bigeard (FSSI)

CERT Santé

Information préalable

Les mesures présentées sont des actions qui nous paraissent “simples et efficaces” à mettre en place avant la période des JOP.

Ces mesures seules ne sont pas suffisantes à la sécurisation d’un système d’information d’un établissement de santé.

Connaitre ses systèmes d'information pour les activités critiques

Identifier les activités critiques pour vos (2 ou 3) activités et les systèmes informatiques (SI) associés et définir :

- **Liste des applications et des services critiques** rendus par l'organisation ;
- **Cartographie des systèmes** sur lesquels les services métiers critiques reposent et sont reliés entre eux ;
- **Cartographie des périphériques** des SI ;
- **Matrice des flux** d'information ;
- **Architectures des réseaux et des éléments fonctionnels**, permettant de faire le lien entre les SI et les processus métiers.
- une liste des **interdépendances des SI entre les métiers et les partenaires extérieurs** (partenaires, sous-traitants, info-gérants, etc.) ;

Identifier la **capacité à fonctionner en mode dégradé** (enclave réseau, papier/crayon…) avec uniquement des services critiques.

Posséder une version hors ligne de ces informations

Recourir à ADS et SILENE

Construire et protéger

Définir une **politique de sauvegarde** en identifiant les données critiques pour l'activité de votre entité.

Considérer les **opérations de sauvegarde et de restauration** comme des opérations sensibles d'administration devant bénéficier **des protections adéquates**

Rendre indépendante l'infrastructure de sauvegarde vis-à-vis des annuaires de production (ex. : Active Directory).

S'assurer du contrôle d'accès des sauvegardes pour garantir qu'elles ne seront ni modifiées ni altérées et toujours disponibles, en particulier dans le cadre de l'utilisation d'offres de sauvegarde cloud.

Chiffrer les sauvegardes au préalable par vos propres moyens pour en cas de solution hors-site

Faire évoluer continuellement l'infrastructure de sauvegarde au même rythme que l'évolution des SI (virtualisation, cloud, etc.) et en fonction de l'évolution de la menace.

Il est recommandé d'appliquer la règle « 3 – 2 – 1 » :
3 copies de la donnée sur 2 supports différents dont 1 hors ligne.

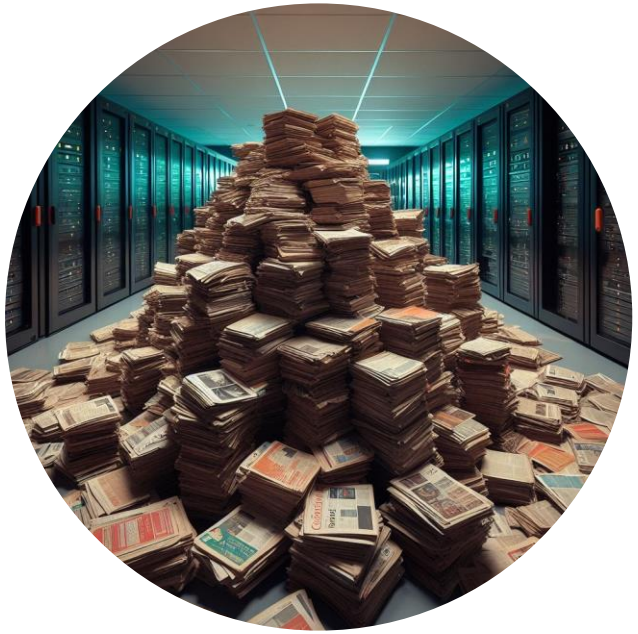
Anticiper et réagir

Définir une **stratégie de restauration**, en lien avec le plan de reprise d'activité et en tenant compte des principaux scénarios d'attaque identifiés sur les SI (rançongiciels, espionnage, etc.).

Réaliser régulièrement des **tests de restauration**.

Ne pas oublier d'inclure **les médias d'installation** et les **configurations des applications métier** dans les sauvegardes.

Prévoir une **procédure d'isolation d'urgence du système de sauvegarde** (serveurs, médias, etc.) en cas de suspicion de compromission ou d'attaque en cours.



Comment ?

Journaliser les events Windows : Windows Event Collector + GPO event forwarding)

Journaliser les équipements périmétriques (Pare-feu, Proxy…)

Augmenter la durée de journalisation autant que possible (6 mois minimum idéalement)

Que faire avec les logs ?

Centraliser les logs

Superviser les alertes de l'antivirus (ou de l'EDR) au minimum une fois par jour

Stocker les logs à froid (hors de l'équipement qui pourrait être compromis)

Anticiper les mesures à prendre en cas de remontée d'alertes (Playbook)

Guide détaillé

Objectif et exemples

Empêcher un attaquant externe d'entrer dans le SI

Quelques exemples récents (Fuites infos / Vulnérabilité critique)

Comment faire ?

Connaître sa surface exposée, et la réduire si possible

Mettre à jour prioritairement les équipements exposés sur Internet

Faire une veille sur les vulnérabilités critiques impactant ses produits

Implémenter des mécanismes d'authentification forte (cf. MFA)

Un bon mot de passe, un bon début.

Un **guide complet** sur les bonnes pratiques (Partie 4 et 5 principalement)

Essayer de se tenir au courant des fuites d'identifiants concernant son établissement (IHaveBeenPwned – LeakCheck – Mozilla Monitor…)

Changer les mots de mot de passe avant les JOP pour éviter l'utilisation d'identifiants ayants précédemment fuités (à qualifier selon établissement)

Avoir une procédure de réinitialisation massive des mots de passe

Utiliser un gestionnaire de mot de passe : 3 mots de passe à retenir, celui de sa session utilisateur, celui de sa session administrateur, le mot de passe maître de son gestionnaire de mot de passe

Une question d'entropie ?

Sup3rm@n1982!

→ On en pense quoi ? (13 caractères et 4 facteurs de complexité)

Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

Sup3rm@n1982!

Your password strength: weak

Estimated time to crack: 1 hour

Sup%B4tWond3r

→ On en pense quoi ? (13 caractères et 4 facteurs de complexité)

Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

Sup%B4tWond3r

Your password strength: strong

Estimated time to crack: 1 month

Source (principalement en cas de cassage à froid)

MFA : Pourquoi ?

Les **accès initiaux** sur des **services exposés sur Internet** ont principalement **2 causes** :

1. **Exploitation d'une vulnérabilité** du service exposé *(voir partie suivante)*
2. **Authentification avec des mots de passe valides** sur le service exposé

   Phishing, Spearphishing

   Guessing, Bruteforce

   Infostealer

   Leak, Compromission d'un site tiers

   → **Mesure de défense : Authentification multi-facteurs (MFA)**

MFA : Où ?

Devant l'entrée du système d'information *(VPN, accès distant VDI, Citrix, etc.)*

Devant une application web *(messagerie, partage de fichiers, application métier, etc.)*

MFA : Comment ?

1. Token physique
2. OTP (token physique ou application)
3. Application (Microsoft Authenticator & Co)
4. Appel téléphonique ou SMS
5. ~~Adresse de messagerie~~

MFA : Difficultés

Logistique (pour les supports physiques)

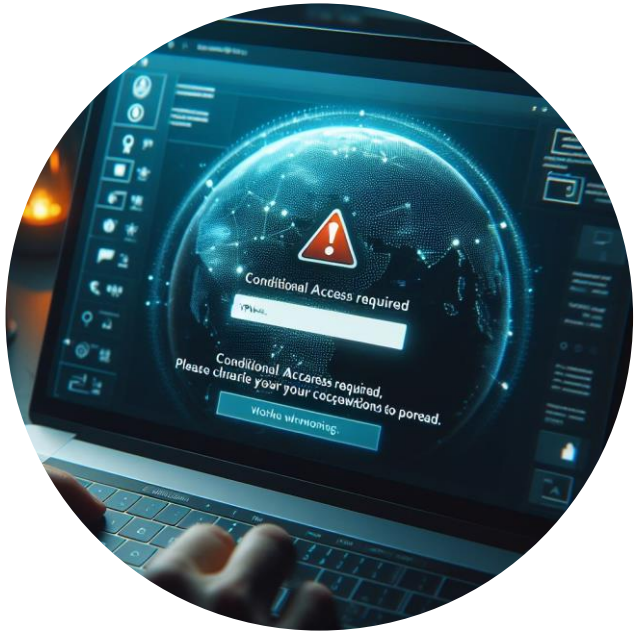
Sphère privée / sphère professionnelle (pour les supports sur portables personnels)

MFA : Avantages

Seul moyen efficace contre l'utilisation illégitime de mots de passe (volés ou devinés)

Evite des incidents et la perte de temps associée (contre la majorité des attaques peu avancées)

Protège l'utilisateur (« responsabilité des actions faites en son nom» « recherche du coupable »)



Qui, Quand, à quoi, comment, depuis où ?

Imposer une authentification forte (MFA - TOTP) **pour tous les accès VPN ou de télémaintenance**

Mettre en place un **ouverte à la demande** pour les accès en télémaintenance avec ses prestataires ayant des droits privilégiés sur le SI

Segmenter le réseau en fonction des groupes de l'utilisateur (faire des groupes (AD / locaux) pour le VPN en fonction des besoins métier)

Contrôler l'accès : Utilisateur légitime / Horaires prévues / Uniquement les machines nécessaires / authentification forte / blocage GeoIP ou IP stricte

Exemple 1 : Groupe secrétaire → GeoIP FR + Horaires 7h – 19h + MFA

Exemple 2 : Télé-mainteneur X → IP éditeur + Fermé par défaut + Accès uniquement aux équipements maintenus + MFA.

Surface d'exposition (C'est comme le soleil , il ne faut pas en abuser)

Pourquoi?

Identifier les composants exposés

Identifier les points d'entrées potentiellement utilisables par des attaquants

Identifier le *shadow IT,* les composants "oubliés" et exposés

Comment?

Pratiquer des scans de ports réguliers et exhaustifs

Utiliser des portails publics référençant sa surface d'exposition

Utiliser des services commerciaux

Limitation

Ne se substitue pas à un audit/test de sécurité

Webinaire CERT Santé sur le sujet

Filtrage

Filtrer les pièces jointes (extensions/types mime)

Filtrer les expéditeurs

Filtrage anti-spam/anti-phishing

Bonnes pratiques

Empêcher l'usurpation de votre identité (DKIM/DMARC/SPF)

Activer le 2FA (pour l'accès aux BAL)

Sensibiliser les utilisateurs (apprendre à reconnaitre une malveillance, hygiène)

Effectuer des vérifications avant toutes modifications d’informations (RIB, adresse transactions bancaires)

Audit

Faire auditer son infrastructure de filtrage de messagerie

Audit de messagerie CERT Santé

Mesures contre la compromission d'un poste de travail

✓ **FILTRAGE WEB :**

(Pourquoi ?) **Entraver la communication au serveur de commande et de contrôle et le dépôt d'outils malveillant**

(Comment ?) Mettre en place une passerelle web sécurisée (proxy) web en *best effort :*

- ✓ *Moteur de réputation IP / domaine*
- ✓ *Catégorisation*
- ✓ *Pas de sortie en IP direct*
- ✓ *Blocage de fichiers téléchargés*
- ✓ *Etc.*

✓ **ANTIVIRUS / EDR (MODE BLOQUANT) :**

(Pourquoi ?) **Entraver le dépôt d'outils malveillant et leur exécution**

(Comment ?)

- ✓ *Déploiement complet sur **TOUT le parc, SANS exception***
- ✓ *Alertes à superviser **minimum une fois par jour**, par une équipe responsabilisée*

Fiche CERT Santé sur les EDR

Mesures contre la compromission d'un poste de travail

✓ DURCISSEMENT SYSTÈME :

(Pourquoi ?) **Entraver l'élévation de privilège et la compromission totale du poste**

(Comment ?)

- ✓ *L'utilisateur ne doit pas être administrateur local de son poste de travail*
- ✓ *Mettre à jour le système et les applications (Outlook, navigateur web, etc.)*
- ✓ *Faire auditer le poste de travail*

✓ PARE-FEU LOCAL :

(Pourquoi ?) **Empêcher l'intrusion par le réseau**

(Comment ?) Sur le pare-feu local : fermer tous les flux entrants

- ✓ *Dans 99% des cas, aucun flux nécessaire sur un poste de travail*
- ✓ *Toute exception doit restreindre les IP sources (flux TV, flux de dépannage utilisateur, autre ?)*

Mesures contre la compromission du domaine

Ségrégation réseau

A minima, réduire l'exposition réseau des systèmes critiques (pare-feu local ou de la zone à protéger)
Restreindre les flux entre les VLANs

Active Directory

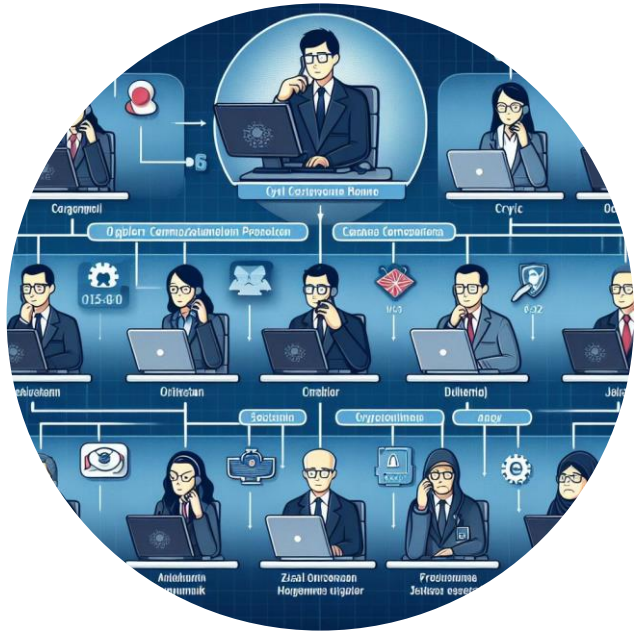
Mise en place de LAPS
Restreindre les droits des comptes génériques (revue de comptes)
Interdire l'adhésion aux groupes Schema admin et Entreprise admin
Réaliser des audits (automatiques et gratuits) de votre AD (ORADAD / PingCastle / Purple Knight…)
Essayer de mettre en place à moyen terme du tiering?

Identifiants

Mettre en place une politique de mot de passe forte **pour tous les comptes**
Mettre en place des mesures anti brute-force / « password spraying » (Fail2Ban complété avec des alertes)

Antivirus

S'assurer de la mise à jour de l'antivirus / EDR et de son déploiement sur **tous** les serveurs - toute exception doit être exclue !



Identifier les parties prenantes des SI

Cartographie des **parties prenantes avec les points de contact** (en particulier si une partie des SI est en sous-traitance) ;

Annuaires à jour des responsables de SI, personnes joignable (et canal pour se joindre) en HO/HNO

Identifier les aides et **prestations de Réponse à Incident** en cas d'incident.

Posséder une version hors ligne de ces informations

Anticiper les attaques par déni de service

Prendre en compte le **dimensionnement** de l'architecture : capacité et redondance

Identifier et **traiter les goulots d'étranglements** (ou SPOF – Single point of failure)

Prendre **contact avec son FAI** (fournisseur d'accès internet) :

- Connaitre les solutions anti-DDoS proposées : coût, délai et intégration
- Identifier des contacts techniques

Fiche DDoS

Entraînez-vous à la gestion de crise cyber

Le kit d'exercice « JOP massifié », spécifiques au contexte des Jeux Olympiques et Paralympiques 2024

Les kits d'exercices crise santé.

CERT Santé

Des questions ?

CERT Santé

Prochain rendez-vous :

16 mai 2024 :

Le CERT Santé propose une session libre de questions-réponses sur la menace cyber, les interventions en réponse à incidents et ses actions de prévention.