AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Intégrer et piloter des prestataires en incident

LA E-SANTÉ FRANÇAISE CERT Santé

Olivier Ruet-Cros
25 juin 2024

TLP : CLEAR

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Sommaire

- Comprendre la problématique
- Rôle et implication des prestataires
- Mesures clés
- Problèmes courants

AGENCE DU NUMÉRIQUE EN SANTÉ

Comprendre la problématique

Périmètre du CERT Santé

Bénéficiaires du CERT Santé

2211 ES* publics
(dont 898 regroupés en 136 GHT*)
1482 ES privés lucratifs
880 ES privés à but non lucratifs

35 000 établissements sociaux et médico-sociaux, centres de radiothérapie, 500 laboratoires de biologie médicale

… au service de plus de
67,8 millions d'usagers citoyens

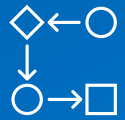
Non bénéficiaires

2M professionnels de santé libéraux
20 000 officines
2 000 centres de santé

ES : Etablissement de soin
GHT : Groupement Hospitalier de Territoire

Comment améliorer le pilotage et l'integration des prestataires au cours d'un incident de sécurité ?

Se préparer



Piloter l'incident

Superviser la sécurité

Choisir son prestataire

Maîtriser le cadre legal et règlementaire

Identifier les types de prestataires

CERT Santé

Infogérants

Production, infrastructure, maintenance, gestion SI

Editeurs

Conception, déploiement, maintenance d'outils, télémaintenance, éditeurs santé, éditeurs de sécurité

Hébergeurs

Hébergement de services, outils, matériels, services reseaux, stockage

Prestataires de sécurité

Conseil, GRC, sécurité opérationnelle , SoC, Pentest, …

Réponse à incidents

Suivi d'incident, analyse inforensique, gestion de crise

A ceci se rajoutent l'ensemble des acteurs et institutions impliquées dans l'incident

Intégration aux étapes d'incidents

CERT Santé

QUALIFICATION	CONFINEMENT	INVESTIGATION	REMEDIATION	DURCISSEMENT
Réaliser une première **évaluation d'un incident** et de ses impacts avérés ou potentiels, et de le partager si nécessaire	Décider et appliquer un ensemble de recommandations pour **isoler une partie du SI**	**Rechercher les origines et les modalités** d'une attaque informatique, ainsi que les éléments du SI qui sont compromis	**Mettre en place les premières mesures** permettant de sécuriser à nouveau le système d'information afin de bloquer l'attaquant	Renforcer la sécurité afin d'**être plus résilient face** à la menace cyber existante
	Infogérants & Hébergeurs Prestataires IR (PRIS) Gestion de crise		Récupération de données SoC	Editeurs Prestataires sécurité Reconstruction

Chaque type de service étant différemment préparé, il est également nécessaire d'anticiper les délais de réaction de chaque prestataire

Mesures clés

Se préparer

CERT Santé

RACI

Définir une **matrice de responsabilités RACI** avec tous les **prestataires** impliqués

Cadre contractuel

Prévoir un volet SSI et incidents dans les échanges contractuels

Ressources et documents

Préparer la documentation SI et définir des protocoles pour y accéder hors SI

Canaux de communication

Définir des canaux indépendants du SI pour pouvoir échanger même en cas d'urgence

Exercices

Inclure les prestataires dans les exercices de préparation

Anticiper en amont la répartition des rôles et responsabilités

Gérer sa documentation

CERT Santé

Technique

Schémas réseaux, **matrices** de flux, **spécifications** d'outils

Contractuelle

Annexes SSI, SLA, **accords** de confidentialité, conventions d'intervention

Annuaire

Carnet d'interlocuteurs, contacts d'urgence, agendas partagés

Opérationnelle

PSSI, fiches réflexes, documentation méthodologique

Conserver un accès partagé à l'ensemble des documents d'incident

Superviser la sécurité

CERT Santé

Processus de développement

Suivre les vulnérabilités publiées par les services de veille

Contrôle des privilèges

Contrôler et suivre les privilèges accordés aux comptes et outils tiers

Segmentation et isolation

Cloisonner les périmètres non gérés par les équipes internes

Infrastructure

Inclure un engagement du prestataire sur le **maintien en conditions de sécurité de son infrastructure**

Identifiants

S'assurer que les identifiants des outils et services tiers sont conformes **à la PSSI et à l'état de l'art**

Suivre et clarifier l'intégration de la sécurité dans les services tiers

S’appuyer sur des référentiels

CERT Santé

Normes de sécurité

Vérifier la conformité aux normes de sécurité : ISO27001, SP800-53, SOC2, …

Cadre règlementaire et légal

Vérifier le cadre règlementaire applicable aux prestataires : LPM 2014-2019, NIS, …

Qualifications de missions

Lister et contrôler les qualifications

ANSSI : PRIS, PASSI, PDIS, …

Valider les services proposés par des qualifications spécifiques

Problèmes courants

La qualité technique

« Ce n’est pas au niveau de ce que j’attendais»

Enjeux

- Garantir la qualité d’analyse
- Valider et appliquer **efficacement** un confinement **adapté**

Mesures

- Clarifier les rôles (contractuellement)
- Prévoir un volet SSI avec son infogérant
- Discuter les résultats fournis

Anticiper l'urgence

« Beaucoup de temps à réagir alors que je suis dans l'urgence»

Enjeux

- **Réduire les délais** de décision et d'action
- Ne pas retarder le passage d'étape d'incident
- **Fludifier** l'échange d'informations

Mesures

- Définir les conditions d'intervention
- Cadrer les possibles déplacements
- Clarifier les créneaux de sollicitation
- Fixer des dates de retour à chaque échange

L’effet « cow-boy »

«Les échanges humains sont difficiles et j’ai le sentiment de ne pas être écouté.e »

Enjeux

- Diminuer la pression globale
- Assurer le partage des résultats
- Maintenir un partage cohérent des responsabilités

Mesures

- Prévoir des réunions physiques
- Définir une cellule de crise dédiée à l’opérationnel
- Maintenir la traçabilité des décisions

Les angles morts

CERT Santé

« Le problème vient d'un périmètre géré par mon prestataire»

Enjeux

- Eviter la sur-compromission liée à un périmètre géré par un tiers
- Eviter la latéralisation vers le reste du SI

Mesures

- Segmenter en amont les périmètres tiers
- Assurer une remontée d'information formelle
- Réduire et encadrer les usages externes sortants de la PSSI

Les rôles

« Je ne sais plus qui fait quoi dans cet incident »

Enjeux

- Ne pas perdre de temps dans les aspects organisationnels
- Ne pas manquer la réalisation des objectifs de crise
- Limiter le flou dans les décisions

Mesures

- S'informer sur les chaînes d'alerte
- Définir une entité responsable de la coordination

Conclusion

Pour résumer : 20 mesures-clés

	Etape	Mesure
1	*Se préparer*	**Organiser une logistique facilitant les échanges directs**
2	*Se préparer*	**Garantir la disponibilité des ressources et documents de crise**
3	*Se préparer*	**Inclure les prestataires dans les exercices de préparation**
4	*Se preparer*	**Définir une matrice de responsabilités RACI avec tous les prestataires impliqués**
5	*Maîtriser le cadre légal et règlementaire*	**Vérifier la règlementation applicable au prestataire :** LPM 2014-2019, NIS, …
6	*Maîtriser le cadre légal et règlementaire*	**Lister les qualifications ANSSI : PRIS, PASSI, PDIS, …**
7	*Maîtriser le cadre légal et règlementaire*	**Vérifier les normes de sécurité : ISO27001, SP800-53, SOC2, …**
8	*Superviser la sécurité*	**Contrôler les privilèges des services et applications tiers**
9	*Superviser la sécurité*	**Cloisonner les périmètres non gérés par les équipes internes**
10	*Superviser la sécurité*	**Inclure un engagement du prestataire sur le maintien en conditions de sécurité de son infrastructure**
11	*Superviser la sécurité*	**Définir des règles de correction de vulnérabilités et des délais de traitement**
12	*Superviser la sécurité*	**Suivre les vulnérabilités publiées par les services de veille**
13	*Piloter l'incident*	**Identifier les acteurs pour chaque étape de traitement de l'incident**
14	*Piloter l'incident*	**Etablir un rythme de fonctionnement précis**
15	*Piloter l'incident*	**Questionner les résultats produits**
16	*Piloter l'incident*	**Accompagner les missions de confinement et d'investigation**
17	*Piloter l'incident*	**Assurer la disponibilité de l'ensemble de la documentation indépendamment du SI**
18	*Sélectionner son prestataire*	**Intégrer des clauses de sécurité opérationnelle, fonctionnelle et technique dans le choix de son prestataire**
19	*Sélectionner son prestataire*	**Définir des conditions de contrôle et d'audit réguliers**
20	*Sélectionner son prestataire*	**Prévoir la gestion des incidents dans le cadre contractuel**

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Questions ?

cyberveille@esante.gouv.fr