FAQ

Webinaire régional d'Ile-de-France Ségur Numérique

« Renforcement de la cyber sécurité dans les établissements sanitaires »

À destination des établissements sanitaires d'Île-de-France, dont tous les établissements opérateurs de services essentiels (OSE)

- 16.12.2022 -

Question 1 : Ne serait-il pas pertinent d'ajouter à ces obligations, le fait de devoir souscrire à un abonnement à un prestataire de réponse à incident de sécurité informatique ? Et le fait d'avoir un SOC ?

Oui cela fait partie des bonnes pratiques, des travaux sont en cours et des propositions seront présentées en 2023.

Concernant les SOC, il existe une offre assez étoffée sur les centrales d'achat nationales. Lors du dernier comité de pilotage SSI, il a été présenté un comparatif des différentes offres à la fois sur le côté technique et financier.
Les offres des centrales d'achat nationales sont abouties et pertinentes. Nous n'avons donc pas estimé nécessaire de lancer un appel d'offres spécifique.

Concernant le prestataire de réponse à incident, nous proposons déjà actuellement ce service en 24/7. Ce service évoluera courant 2023 par la sélection d'un nouveau prestataire.

Question 2 : Je comprends la pertinence que la direction soit présente lors de l'exercice, mais ce ne sera pas nécessairement aussi confort/ le cas lors d'une attaque cyber. N'est-ce pas pertinent de tester aussi la façon de s'y prendre en cas d'absence de la direction ?

Un des objectifs de ces exercices est de sensibiliser les directions, d'où l'importance de leur présence et de leur implication dans cette démarche.

Question 3 : Vous parlez d'un SOC opéré?

Oui nous parlons de SOC opéré : c'est-à-dire externe. Parmi les SOC opéré nous en avons identifié 4 de disponibles via la CAIH ou le RESAH. Certains établissements ont déjà souscrit à des offres de leur côté. Un SOC opéré est extrêmement important puisque si des alertes sont relevées, mais pas traitées, cela peut présenter un risque important pour la structure.

Question 4 : Le SESAN est-il en relation avec les DSI de groupes d'établissements ?

Pas à notre connaissance, mais SESAN se tient à la disposition de ces DSI pour initier des échanges. N'hésitez pas à contacter ssi@sesan.fr pour toute demande d'information complémentaire, une réponse vous sera donnée rapidement.

Question 5 : Quelle a été l'attaque du CH Versailles ? Ransomware ?

Oui cela a été un rançongiciel, des enquêtes sont en cours pour déceler l'origine de cette attaque.

Question 6 : Le fait que mon établissement n'a fait aucun audit depuis 2 ans peut empêcher d'avoir un financement ?

Non cela ne fait pas parti des prérequis, vous pourrez obtenir un financement dans la mesure où vous renseignez le formulaire de candidature sur démarches simplifiées et que vous respectez les prérequis à savoir :
- Avoir passé commande auprès d'une entreprise
- Avoir renseigné l'OPSSIES dans un délai de 3 mois maximum
- Avoir renseigné la grille de maturité et vous être positionné sur l'une des 3 catégories

Question 7 : Quelles sont les vulnérabilités types qui font que les attaques par ransomware réussissent ?

Pour qu'une attaque par rançongiciel réussisse, il faut une porte d'entrée qui peut être, par exemple :
- Un accès au SI non surveillé : par exemple, un prestataire qui se serait fait hacker et qui permet donc à un hackeur de rentrer dans le SI de l'établissement
- Du phishing : si les salariés indiquent leurs identifiants/login et mots de passe en réponse à un mail de phishing, ce qui permet à un hackeur d'avoir les éléments pour faire un premier pas dans le système d'information et après élever ses privilèges en profitant des failles possibles sur l'AD.

Question 8 : Pouvons-nous prétendre à plusieurs financements ? Pour plusieurs solutions ?

Non, l'enjeu de cet AAP est de financer un seul exercice de continuité d'activité en mode dégradé, au cours de l'année 2023. Pour rappel, l'objectif de cet exercice est la mise en place d'un plan d'action permettant de prévenir les crises et de pallier aux failles éventuelles des systèmes d'information.

Question 9 : Vous parlez de continuité d'activité alors que les Kits parlent en premier lieu d'entrainer la cellule de crise, ai-je mal compris?

On parle d'exercice de cyber crise, mais suite à un exercice de cyber crise on parle de continuité d'activité donc cela va déclencher soit la rédaction d'un plan de continuité d'activité soit l'utilisation du plan de continuité qui aura été défini au préalable.

Plus précisément, quand on parle de "continuité d'activité" ce n'est pas de la continuité d'activité technique du SI à proprement parler dont il est question, mais plutôt de la continuité, en l'absence de fonctionnement du SI, d'un service de prise en charge du patient, des services des ressources humaines, etc.
En parallèle, doit être résolue la crise technique.

D'où la nécessité d'impliquer les directions dans ces exercices puisque celle-ci va, dans sa globalité, travailler à la fois sur la coordination des moyens techniques et/ou humains voir financiers nécessaires à la résolution de la crise technique et sur le maintien de la prise en charge des patients et du fonctionnement de l'établissement.

Question 10 : On ne parle pas de tester le PCa en conditions réelles ?

Non, on ne teste pas le Pca en conditions réelles, c'est une simulation. On n'injecte pas un vrai rançongiciel dans le système d'information pour évaluer la réaction de la cybercrise et s'assurer que les procédures sont connues et bien impliquées.

Question 11 : Quand vous parlez de "bastion de protection sécurité", vous pensez à la solution BASTION ou vous êtes plus général ? Cette dernière me semble représenter une charge élevée à notre équipe SI

On parle bien ici de Bastion d'administration. Pour l'équipe SI ce serait un élément facilitateur plutôt qu'une charge. Puisqu'au lieu de devoir se connecter à l'ensemble des équipements pour effectuer ses tâches d'administration, l'équipe SI passerait par un même Bastion pour effectuer la connexion.
Nous utilisons ce système au sein de SESAN et son utilisation est bien plus simple que la connexion par authentifications individuelles à chaque serveur. De plus, le Bastion permet d'enregistrer la session, de vérifier si des erreurs ont été commises et de pouvoir restaurer et réparer bien plus facilement.
Cela permet aussi de maîtriser les accès des prestataires.