AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Charte d'audit de cyber-surveillance

Evaluation de la sécurité des domaines exposés sur Internet

Statut : Validé | *Classification : Publique* | *Version : v2.3*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. AUDIT DE CYBER-SURVEILLANCE A DESTINATION DES STRUCTURES DE SANTE

La ministre des solidarités et de la santé a transmis aux directions des établissements de santé de référence un plan de renforcement de la cybersécurité. Un audit de l'exposition sur Internet de l'ensemble des systèmes numériques est exigé dans le cadre de la phase de diagnostic. A ce titre, la mise en œuvre progressive au niveau national d'un service de cyber-surveillance est prévue dans le cadre de l'action 9 de la feuille de route #Ma santé 2022.

Par ailleurs, le prérequis PS2.2 du programme SUN-ES demande la réalisation d'un audit externe de cyber-surveillance. Le rapport issu du service de cyber-surveillance de l'ANS est reconnu comme document de preuve pour l'atteinte de cet indicateur.

Cet audit est réalisé à titre gracieux par l'ANS sur les domaines précisés dans le formulaire d'engagement au respect de la charte signé (ci-après dénommé « le formulaire d'engagement ») par la structure de santé et l'ANS.

1.1. Nature et déroulement de l'audit

L'ANS réalise un audit des domaines de la structure de santé (ci-après dénommée la structure) exposés sur Internet et mentionnés dans le formulaire d'engagement susmentionné, afin d'en évaluer le niveau de sécurité et de détecter d'éventuelles vulnérabilités.

L'audit se déroule en deux phases :

- Une phase passive consistant en la collecte d'informations à partir de sources ouvertes sur Internet ;
- Une phase active consistant en la réalisation d'un audit de chacun des domaines du système d'information de la structure. Cette phase comprend :
    - Une cartographie des services et des ressources accessibles ;
    - Le test des comptes avec des identifiants faibles et des identifiants par défaut ;
    - L'utilisation des scanneurs généralistes / spécifiques afin de détecter d'éventuelles erreurs de configuration et / ou de défauts de mise à jour.

Contrairement à un test d'intrusion, il est à noter que lors de cet audit, les vulnérabilités pouvant présenter un risque pour la disponibilité ou l'intégrité du système ou des données ne sont pas testées (exemple : déni de service).

Du fait de l'automatisation quasi-totale des tests, certaines informations collectées peuvent nécessiter une validation manuelle afin d'éviter les faux-positifs et de confirmer la présence effective d'une vulnérabilité.

Afin de garantir un bon déroulement de l'audit, il est suggéré aux structures de surveiller les domaines audités durant les phases de tests.

Le détail de la méthodologie utilisée est précisé en annexe 2.

Un rapport présentant les vulnérabilités identifiées, leur niveau de criticité et des mesures correctives est produit par l'ANS à l'issue de l'audit puis communiqué à la structure.

La structure s'engage à faire un retour d'expérience à l'ANS sur le contenu du rapport, les bénéfices de l'audit et les éventuels points d'amélioration.

1.2. Autorisation de réalisation des tests

La structure autorise l'ANS à procéder aux tests dans les conditions définies à l'article 1.2 de la présente charte et à l'annexe 2.

Cette autorisation couvre notamment les tests réalisés sur les infrastructures sous maitrise de la structure. La structure peut avoir fait le choix d'externaliser tout ou partie de son système d'information. Dans ce cas, elle s'engage à informer et obtenir l'autorisation de son prestataire préalablement à la réalisation des tests.

De plus, sous réserve de l'autorisation préalable de la structure, l'ANS se réserve le droit d'exploiter certaines vulnérabilités afin d'établir une liste de ses impacts potentiels. L'autorisation de la structure est demandée par e-mail, à l'adresse de contact indiquée dans le formulaire d'engagement.

2. CONFIDENTIALITE

Seuls les services du HFDS, les personnes impliquées dans l'activité de cyber-surveillance au sein de l'ANS et l'ANSSI auront connaissance du rapport d'audit. Néanmoins les résultats non détaillés des rapports d'audits pourront être partagés à l'OPSSIES (Observatoire Permanent de la Sécurité des Systèmes d'Information des Établissements de Santé) à des fins statistiques.

Les données collectées pour réaliser le rapport sont conservées trois mois après la production de celui-ci afin de pouvoir, à la demande de la structure, réaliser une analyse approfondie d'une ou plusieurs vulnérabilités identifiées.

3. PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de la réalisation de l'audit, l'ANS, qui agit pour le compte et sur instruction de la structure, est susceptible de collecter, de manière accessoire, des données à caractère personnel qui auraient fait l'objet d'une fuite de données. Les données ainsi collectées ne sont pas intégrées au rapport et ne sont pas transmises à la structure de santé. Comme toutes les données collectées lors de l'audit, elles sont conservées par l'ANS pour une durée de trois mois après la production du rapport afin de pouvoir, à la demande de la structure, réaliser une analyse approfondie d'une ou plusieurs vulnérabilités identifiées. Les personnes concernées sont informées par la structure de santé, dans le cadre de l'information faite pour la mise en œuvre des traitements relevant de l'exécution de ses missions. L'exercice des droits se fait auprès de la structure de santé, de même que la procédure éventuelle de signalement.

Annexe - Présentation de la méthodologie utilisée

Il est à noter que l'ensemble des tâches est réalisé par une plate-forme chargée de la collecte, de l'analyse et de la restitution d'informations récupérées à partir de sources ouvertes et de techniques avec de faibles contacts directs (sans exploitation offensive).

Les différentes phases

Phase 1 : Récupération d'informations

Cette étape consiste à collecter toutes sortes d'informations techniques sur la cible :

- De manière publique :
  - à partir des sites référençant le domaine surveillé ;
  - à partir de recherches Google customisées (Google Dork, GoolaG) ;
  - à partir des informations des sites du domaine audité ;
  - à partir des informations publiques de noms de domaines et d'hébergement.
- De manière ciblée:
  - en testant les services ouverts (WWW, Mail, FTP, DNS, News, LDAP, etc.) ;
  - en étudiant le code source des pages des sites Web ;
  - en utilisant des particularités protocolaires réseaux (divers traceroute, ping avec options, etc.).
  - en utilisant des scanners de ports TCP/UDP ;
  - en utilisant des scanners applicatifs (HTTP, FTP, etc.) ;
  - en utilisant des outils réseaux spécifiques (Nessus, Whisker, nikto, etc...).

Cela permet de déterminer un premier niveau de cartographie des services et ressources Internet à auditer.

Phase 2 : Analyse des informations recueillies

Le but de cette étape est d'identifier le plus précisément possible les services ouverts sur Internet (messagerie, DNS, serveur FTP, serveur Web, VPN, etc.), les serveurs hébergeant ces services, les versions de logiciel installées sur ces serveurs.

Pour faire suite à l'établissement de la « cartographie », une recherche de toutes les vulnérabilités potentielles liées à chaque service en ligne est réalisée.

Les recherches sont réalisées au moyen :

- des informations fournies par les serveurs Web ;
- pour les CMS, des composants (plugins, thèmes, widget…) utilisés pour identifier le type et la version (Wordpress, Drupal, EZpublish…) ;
- des outils de scan de ports (Nmap, Superscan, etc.) ;
- des scanners de vulnérabilités généraux ou spécifiques (Nessus, Nikto, etc.) ;
- des outils propriétaires développés sur mesure pour ce type d'audit sécurité.

Les tests permettent notamment d'identifier :

- des vulnérabilités en conception (conception du produit ou du protocole) ;
- des vulnérabilités en exploitation (configuration du produit, utilisation, mise à jour).

Aucun test agressif (débordement de tampon mémoire, dénis de service, attaque par dictionnaire pouvant entraîner le blocage d'utilisateurs) n'est effectué dans le cadre de l'audit.

Néanmoins dans certains cas particuliers et sous réserve de l'autorisation préalable de la structure, l'ANS se réserve le droit d'exploiter certaines vulnérabilités afin d'établir une liste de ses potentiels impacts.