HOSPITALIER

La Couronne / 16

SRC SOLUTION

Centre Hospitalier Camille Claudel
Test d'intrusion du Système d'information

Client
Centre Hospitalier Camille Claudel

Capacité
259 lits

Effectif total
961 personnes

Budget d'exploitation
54 M€

Caractéristiques de la prestation SRC

- Type : Audit Sécurité / Test d'intrusion
- Durée audits : 3 mois
- Durée accompagnement : 2 ans
- Profil : Consultant Sécurité des SI

Le projet

Le Centre Hospitalier Camille Claudel a souhaité réaliser un état des lieux exhaustif du niveau de sécurité atteint par son dispositif anti-intrusion.

La mission consistait à procéder à une analyse de l'infrastructure des systèmes d'information et des réseaux. Cette analyse devait faire apparaître les failles et risques conséquents d'intrusions actives et d'intrusions virales ou automatisées.

Cette prestation devait se dérouler avec comme fil rouge le maintien en condition opérationnel du système d'information en n'effectuant aucune action pouvant nuire au système d'information du Centre Hospitalier.

A la demande de la direction des systèmes d'information du Centre Hospitalier le document livrable rendrait compte des opérations d'audits effectuées et intègrerait un recueil des anomalies constatées lors de chaque phase d'audit (BlackBox, GreyBox, WhiteBox) devant faire l'objet d'un traitement immédiat compte tenu le cas échéant, du caractère grave et urgent de celles-ci.

Le projet a été divisé en 2 Phases et une option :

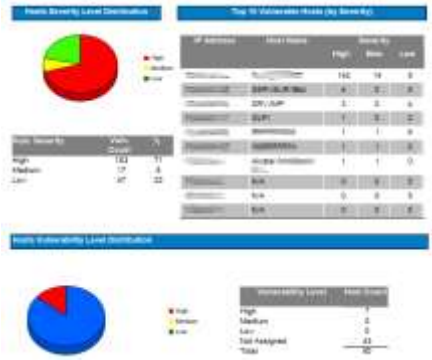
- Phase 1 : Réunion de cadrage
- Phase 2 : Audits terrains :
  - Audit organisationnel et technique,
  - Audit des vulnérabilités et intrusions,
  - Audit de configuration
- Option : Accompagnement post-audit.

Points marquants du projet :

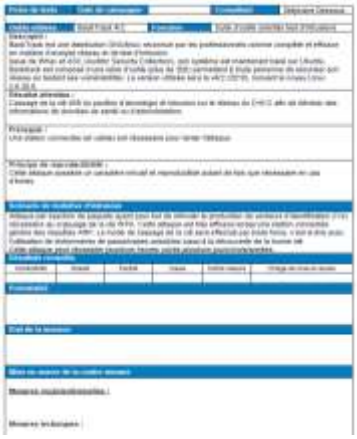
Lors de cette mission, il s'est avéré que tenter l'intrusion pure des systèmes était inutile dans certains cas compte tenu du manque d'implémentation de moyens de sécurité au sein du Centre Hospitalier. En effet, concernant la protection périmétrique du centre vis-à-vis de l'internet, bien que le moyen mis en œuvre soit d'une qualité et d'une fiabilité éprouvée, l'architecture et les usages en vigueur nous ont permis pendant cette phase d'audit de pouvoir observer une intrusion réelle du serveur de messagerie impliquant un arrêt du service au moins égal à 5 jours. Cet incident de sécurité à mis en évidence dès le début de la prestation les axes d'efforts sur lesquels le Centre Hospitalier devait se concentrer dans les jours, semaines et mois à venir. L'intrusion en question portait sur le serveur de messagerie du centre hospitalier et émanait du continent asiatique.
Un projet vaste, mêlant différents types d'audits techniques sur le système d'information, avec une partie d'analyse post-intrusion non prévue préalablement suite à incident.

Origine de l'attaque du serveur de messagerie :

Exemple de tableau de bord de vulnérabilités :



Exemple fiche de test d'intrusion wifi :



Planning :

- Phases d'audit : 07/2011 à 09/2011,
- Phase post-audit : 09/2011 à 02/2013