TESTS D'INTRUSION, MAÎTRISE TECHNIQUE ET SENSIBILISATION AUX BONNES PRATIQUES

CYBER-SÉCURITÉ : GPLEXPERT PREND POSITION

Marquée par la multiplication des cyber-attaques visant les établissements de santé, la récente crise sanitaire a mis en lumière l'importance primordiale des bonnes pratiques de sécurité informatique, sur le plan technique comme humain. Grégory Rochette et Sébastien Suard, consultants pour le cabinet de conseil en e-santé GPLExpert, nous en disent plus. **Par Joëlle Hayek**

POUR QUELLES RAISONS LES ÉTABLISSEMENTS DE SANTÉ ÉTAIENT-ILS PLUS VULNÉRABLES AUX CYBER-ATTAQUES DURANT LA CRISE SANITAIRE ?
GRÉGORY ROCHETTE : Depuis toujours les établissements de santé ont des besoins légitimes d'accès à l'information de manière instantanée. Parfois au détriment des règles de base en matière d'authentification. Les tentatives de piratage informatique ont été favorisées par la mise en œuvre du télétravail dans l'urgence durant la période de confinement. Les réseaux et pare-feux des établissements de santé étaient en effet parfois sous-dimensionnés, ce qui a permis aux cyber-pirates de trouver de nouvelles portes d'entrées, a fortiori lorsque les utilisateurs n'étaient pas formés aux bonnes pratiques de sécurité informatique. Nous avons donc assisté à la recrudescence des attaques par déni de service, des tentatives de prise en main à distance des équipements vulnérables, mais aussi des attaques de type phishing ou par dictionnaire.

QUELLES BONNES PRATIQUES PRÉCONISEZ-VOUS POUR S'EN PRÉMUNIR ?
SÉBASTIEN SUARD : Outre le déploiement d'équipements capables à la fois de prévenir et de détecter les intrusions, il faut en premier lieu sensibiliser les utilisateurs, qui sont à l'origine de la majorité des failles : vérification des URL, mots

> “LES *PENTESTS* PERMETTENT À UN AUDITEUR EXPÉRIMENTÉ DE SE METTRE **DANS LA PEAU D’UN HACKEUR À LA RECHERCHE DE VULNÉRABILITÉS SUR LE SYSTÈME D’INFORMATION”**

de passe robustes, déconnexion systématique, etc. Il y a ensuite deux règles d’or : n’ouvrir vers l’extérieur que les applications qui doivent impérativement l’être et effectuer des mises à jour régulières. Nous recommandons de réaliser, en parallèle, des *Pentests*, ou tests d’intrusion, entre une et deux fois par an, pour identifier les vulnérabilités des services et des serveurs exposés sur Internet.

EN QUOI CONSISTENT PLUS CONCRÈTEMENT CES *PENTESTS* ?
GRÉGORY ROCHETTE : Les *Pentests* permettent à un auditeur expérimenté de se mettre dans la peau d’un hackeur à la recherche de vulnérabilités sur le système d’information cible. Nous commençons par définir le périmètre et la période de réalisation du test, puis, une fois l’audit effectué, nous rédigeons un rapport détaillant les différentes vulnérabilités découvertes, leur exploitabilité et surtout leur degré de criticité pour l’activité de l’établissement. Un *Pentest* doit donc à la fois être effectué sur un périmètre identique à celui du test précédent, pour vérifier la pertinence des nouvelles mesures de sécurité, et sur un périmètre différent pour tester d’autres serveurs et services. Les *Pentests* font d’ailleurs désormais partie des prérequis du programme HOP’EN, et devraient être également intégrés à la future certification HAS des systèmes d’information hospitaliers (SIH).

SÉBASTIEN SUARD : Mais il est possible pour un établissement d’aller plus loin, en doublant ces tests d’intrusion externes par des tests d’intrusion internes, qui consistent à auditer le système d’information hospitalier sur les plans physique (locaux), humain (utilisateurs) et technique (outils). Ces deux approches combinées représentent ce que l’on appelle l’audit sécurité. Il existe également d’autres types de tests, comme l’audit d’ingénierie sociale, pour par exemple vérifier l’imperméabilité des utilisateurs aux pratiques de *phishing.* Toutes ces options sont proposées par GPLExpert.

VOUS L’AVEZ ÉVOQUÉ, LA SÉCURITÉ INFORMATIQUE VA AU-DELÀ DU VOLET TECHNIQUE, PUISQU’ELLE A UNE LARGE COMPOSANTE HUMAINE. POUVEZ-VOUS NOUS EN PARLER ?
SÉBASTIEN SUARD : Il faut en effet un chef d’orchestre, dans l’idéal un responsable de la sécurité du système d’information (RSSI). Mais cette fonction-clé est relativement rare dans les établissements de santé, qui disposent plutôt d’un référent de la sécurité du SI. Son rôle est moins technique qu’organisationnel et managérial : il fait le lien entre la direction, les utilisateurs et les techniciens, accompagne la conduite du changement, etc. GPLExpert propose ici un accompagnement spécialisé pour lui permettre justement d’acquérir des compétences techniques, sur l’analyse et l’évaluation des risques, l’élaboration d’un plan d’actions… Pour les établissements qui le souhaitent, nous proposons également une prestation de RSSI externalisé.

LE MOT DE LA FIN ?
GRÉGORY ROCHETTE : Beaucoup d’établissements vont aujourd’hui vers la cybersécurité en raison d’une unique obligation légale – ou parce qu’ils ont déjà été piratés. C’est pourtant un enjeu réel, et vital pour éviter toute paralysie des services de soins ainsi que toute perte ou divulgation des données, souvent sensibles. Il ne faut donc pas hésiter à réaliser ou à se faire accompagner afin d’obtenir une vision claire des vulnérabilités, en menant, par exemple, des tests d’intrusion avant que d’autres ne les identifient pour vous, de manière malveillante… ●

Fiche RSSI

Acteur incontournable de la sécurité, le RSSI est un interlocuteur privilégié entre la direction et les utilisateurs du système d’information. Il participe à l’élaboration et veille au respect des règles et des référentiels de sécurité de l’établissement. En fonction de ses compétences et de ses responsabilités le RSSI peut être nommé « Responsable » ou « Référent » de la Sécurité du Système d’Information et participer aux missions suivantes :

- **Sensibilisation et communication** auprès de la direction et des utilisateurs
- **Évaluation et traitement des risques** liés à la sécurité du SI
- **Pilotage et gestion de projet SI** pour anticiper les éventuels risques techniques, humains, organisationnels et juridiques
- **Mise en œuvre de solution techniques** de détection et de protection contre les attaques informatiques
- **Gestion des incidents de sécurité du SI** en liaison avec la DSI et le DPO
- **Audit et contrôle** des exigences de sécurité et des référentiels applicables
- **Veille technologique et juridique** en continu dans un objectif d’anticipation des risques.

Les conseils de Damien Ribeiro, RSSI chez GPLExpert : « *Pour que son positionnement soit légitime et qu’il puisse atteindre les objectifs de sécurité de son entreprise, le RSSI doit :*
- Être formé et accompagné dans l’exercice de ses fonctions
- Obtenir un soutien de la direction
- Disposer d’une fiche de fonction cohérente avec son quotidien
- Bénéficier d’un temps dédié à ses missions. »