CONCLUSIONES

Durante el tiempo en el que me desempeñé como analista de incidentes y de cómputo forense en el UNAM-CERT, identifiqué como las causas principales de accesos no autorizados en RED-UNAM, el uso de contraseñas inseguras y la incorrecta administración de las mismas. A fin de contribuir a mitigar esta vulnerabilidad, realicé los manuales de implementación de contraseñas robustas con cracklib y passwdqc, que son herramientas gratuitas para incrementar de manera significativa la seguridad de las contraseñas en los sistemas de cómputo con sistema operativo GNU/LINUX.

Tomando en cuenta que no sólo es importante generar manuales de seguridad de la información, sino también establecer una estrategia para difundirlos y mantenerlos vigentes, busqué el mejor medio para darlos a conocer a la comunidad de administradores de RED-UNAM.

Varios años antes de mi incorporación a la organización, el UNAM-CERT organiza anualmente el evento "Admin-UNAM", el cual es un seminario que tiene como finalidad fortalecer la colaboración en materia de seguridad de la información entre las dependencias de la UNAM así como discutir e instrumentar soluciones ante los problemas y retos de esta índole que se presentan en nuestra universidad.

Aprovechando que la finalidad del seminario es acorde con los objetivos de los manuales de seguridad que elaboré, sugerí que el portal del evento ADMIN-UNAM se modificara para no fuera sólo un sitio informativo, sino un portal que permitiera hacerle difusión a los manuales y al mismo tiempo, obtener retroalimentación de los usuarios para mantenerlo siempre vigente, ajustándolo a las necesidades cambiantes de los usuarios. El jefe del área de atención a incidentes, el subdirector de seguridad de la información y mis colaboradores de atención a incidentes apoyaron y enriquecieron mi propuesta con sus propias ideas.

Así, se sentaron las bases para que no sólo personal con conocimientos especializados de UNAM-CERT tuvieran un medio para compartir sus conocimientos en materia de seguridad informática con los administradores de RED-UNAM, sino para que los propios administradores de RED-UNAM aportaran sus conocimientos y experiencia a otros administradores.

El manual de notificación y prevención de correo fraudulento, ha sido un recurso de información fundamental en la operación diaria del equipo de respuesta a incidentes de UNAM-CERT. Antes de su elaboración, era necesario explicarle a muchos usuarios cómo notificarlos correctamente, lo que reducía nuestro tiempo de respuesta. Después de la elaboración y difusión de este manual, notamos que la cantidad de usuarios que proporcionó sus credenciales de acceso se redujo y que la notificación de este tipo de eventos al equipo de respuesta a incidentes de UNAM-CERT mejoró.

La misión del UNAM-CERT para con la máxima casa de estudios es proporcionar servicios de asesoría y atención a incidentes en materia de seguridad informática a cada una de las dependencias que la conforman, satisfaciendo sus necesidades con base en la capacidad

tecnológica que se disponga. Para cumplir con ello, es fundamental que el personal de atención a incidentes pueda acceder rápidamente a la información de contacto actualizada de los responsables de las entidades de la UNAM, para que en caso de registrarse un incidente de seguridad, éste pueda ser notificado al responsable de la red de datos donde ocurrió para se realicen oportunamente las acciones para contener y erradicar el incidente y así reducir el impacto de la amenaza de seguridad.

El servidor whois fue fundamental para cumplir con este objetivo, no sólo porque permitió acceder más rápidamente a la información de contacto de administradores de redes de RED-UNAM y de equipos de respuesta a incidentes de otros países, sino porque funciona como un sistema alterno en donde se puede consultar la información en caso de que el Sistema de Atención a Incidentes pierda disponibilidad. Así, es una pieza clave en el plan de continuidad del proceso de atención a incidentes, uno de los procesos más importantes para el UNAM-CERT.

El tiempo de respuesta es uno de los aspectos más importantes para un CERT. Entre más breve sea, el impacto causado por la amenaza de seguridad será menor y por lo tanto, se protegerán mejor los activos de la organización.

Además, el servidor whois permite compartir la información con dependencias externas por medio de un cliente whois. Así, el personal del Departamento de Redes de la DGTIC puede acceder a la información de contacto actualizada de administradores de RED-UNAM y así identificar y resolver más rápidamente problemas con la red de datos.

Como señalan las buenas prácticas de ingeniería de software, al elaborar un sistema hay que tomar en cuenta las amenazas que pueden afectarlo a fin de tomar las acciones para corregirlas o al menos detectarlas y notificarlas oportunamente. Específicamente durante la elaboración del servidor whois realicé modificaciones en el código fuente para detectar y notificar las siguientes situaciones:

- Que el archivo con la información de administradores de RED-UNAM, enviado desde el Sistema de Atención a Incidentes no llegara o estuviera vacío.
- Pérdida de disponibilidad de la red de datos.
- Pérdida de disponibilidad del servidor de correo.

A lo largo del ejercicio de mi profesión, observé en varias ocasiones que los sistemas que no estaban documentados o que tenían documentación incompleta o confusa se dejaban de utilizar y se optaba por desarrollar nuevos sistemas desde cero. También observé que los sistemas que cambiaban de desarrolladores, en muchas ocasiones tenían código innecesario, lo que provocó que éstos fueran ineficientes y que fuera complicado modificar el código realizado por un antiguo desarrollador. Para reducir este problema, es fundamental fomentar en el estudiante de ingeniería en computación las habilidades necesarias para documentar correctamente sus acciones, apegarse a las buenas prácticas y modificar los sistemas elaborados por otras personas.

Durante el transcurso de la carrera, es habitual que el estudiante desarrolle programas o aplicaciones desde cero, realizando todas las fases de ingeniería de software, análisis de requerimientos funcionales y no funcionales, análisis y diseño de arquitectura, implementación, instalación y mantenimiento. Sin embargo, en muchos entornos reales de producción, debido a limitantes de tiempo, o a que se tienen sistemas existentes, es necesario modificarlos. Esto supone en ocasiones un reto adicional, ya que hay que entender la manera de pensar, diseñar y programar de otras personas y ser capaz de modificar los sistemas existentes para satisfacer las necesidades de la organización y cumplir con los objetivos propuestos.

A fin de fomentar esta habilidad, yo propongo que desde los primeros semestres de las asignaturas de programación se haga énfasis en las buenas prácticas y no sólo a que los programas funcionen. Es fundamental que el alumno entienda la importancia del uso de estandarización, la claridad, los comentarios en el código fuente y la documentación suficiente y clara. Las buenas prácticas son necesarias porque, entre otras cosas, permiten a los actuales desarrolladores entender más rápidamente los sistemas desarrollados por otros y así modificarlos más fácilmente en caso de ser necesario.

Sugiero que en la Facultad de Ingeniería se asignen proyectos que tengan como propósito modificar proyectos de software realizados por otros alumnos, a fin de evaluar la capacidad del alumno de adecuarse a un sistema existente y sujetarse a lo ya establecido por los autores del sistema. Este ejercicio puede ser una práctica excelente para mostrar la importancia de las buenas prácticas en el software y de la necesidad de contar con documentación suficiente, actualizada y útil de los sistemas desarrollados.