Ataques a la seguridad de la red de telecomunicaciones del Instituto

Durante las tres últimas semanas del pasado mes de marzo, la red telecomunicaciones del Instituto de Ingeniería sufrió severos ataques informáticos, lo que trastornó en forma seria el trabajo académico y administrativo de nuestra entidad. Por la trascendencia y por ser un hecho sin precedentes, vale la pena destinar este espacio, normalmente dirigido a temas académicos, a comentar sobre esa situación.

De hecho, el primer ataque se dio el 13 de febrero y fue controlado hasta el 21 del mismo mes. El problema se presentaba con patrones regulares que coincidían con la jornada laboral, y que incluso desaparecieron el fin de semana. Con apoyo del personal de seguridad de la Dirección General de Cómputo y de Tecnologías de la Información y Comunicación (DGTIC) y del fabricante Hewlett Packard, proveedor de equipos importantes de nuestra red, pudimos identificar la suplantación del *firewall*, y con ello, el impedimento de comunicación de nuestra red con Internet. La evaluación llevó a relacionar el problema con el servicio de VPN, el cual fue suspendido, y con ello fue resuelto el caso.

Posteriormente a ese evento, la Coordinación de Sistemas de Cómputo continuó con el monitoreo, el análisis de tráfico y la revisión de intentos de intrusión en diferentes puntos de la red. En esa acción se detectó una actividad anormal permanente en la intensidad del tráfico y del número de intentos de conexión de un programa de cómputo del servicio en la nube (red de cobertura mundial) denominado Teamviewer, instalado por los usuarios en varias computadoras del Instituto, fundamentalmente en dos coordinaciones. Este programa evade protecciones de seguridad de la red mediante túneles encriptados y permite el control de una computadora interna desde el exterior. La revisión de algunos de estos equipos llevó a identificar varios problemas del llamado "*software* malicioso" (caballos de Troya, puertas traseras, etc.).

El segundo ataque, diferente al primero y de mayor envergadura, se presentó a partir del 12 de marzo y se prolongó prácticamente por el resto del mes, causando, sin duda, graves problemas a todos los usuarios. En esta ocasión, y por la fuerza del ataque, se incorporó al equipo de apoyo a los especialistas de seguridad y redes de las empresas Microsoft México, Hewlett Packard, Quatro Networks (Cisco) y Websense. Esta acción, claramente malintencionada, bloqueó nuestros servidores, particularmente los que nos dan la salida a Internet. Incluso, un equipo de cómputo especializado en la detección y el bloqueo de intrusos (TippingPoint) quedó comprometido al ser intervenido en forma externa, lo que evitó su función de protección.

La decisión tomada durante ese periodo fue reconfigurar y reforzar la zona perimetral de seguridad de la red, actualizar el núcleo de la red y reubicar los servidores Windows y Linux (pumas e iingen en otros) a una subred con mayor seguridad. Por su parte, el monitoreo de tráfico y la detección de intrusiones se mantienen activos.

Es importante señalar que los trabajos realizados por las empresas de apoyo permitieron constatar que los equipos, los programas y las capacidades técnicas del personal no fueron la causa de las fallas en la red. Estas fueron debidas, al menos en el primer ataque, a que la seguridad de varias computadoras de usuario fue comprometida. La vulnerabilidad se presentó en la estructura de la red que operó durante varios años sin problemas, pero que no pudo detectar ni contener los ataques en esta ocasión. Tal conclusión lleva a la necesidad de revisar este aspecto, tanto en la adecuación de su estructura como en la actualización de ciertos equipos que tienen varios años de operación y que no son ya adecuados para una red con mayor seguridad. Igualmente, será necesario revisar y redefinir las políticas de uso de la red, particularmente lo relacionado con la descarga de *software* y el uso de la red para actividades no académicas, así como con la incorporación de equipos que no pertenecen a la UNAM.

La Coordinación de Sistemas de Cómputo, la Subdirección de esa área, la Secretaría Académica y la Dirección tienen claro que tener una red de telecomunicaciones segura, funcional y de última tecnología es indispensable para el trabajo académico de este instituto. En este contexto y para mantener una red con niveles altos de seguridad, confiabilidad y disponibilidad se requiere la participación permanente y vigilante de toda la comunidad.

La enseñanza que nos deja este inesperado episodio llevará a tomar acciones en el corto plazo para que no se vuelva a presentar. Los usuarios de esta infraestructura, tanto académicos como administrativos y estudiantes, además de algunas asociaciones gremiales con convenio, no deben perder la confianza en los altos estándares de desempeño que la caracterizaba hasta antes de los ataques mencionados. Para ello, trabajaremos en las próximas semanas.

Adalberto Noyola Robles
Director