PERIÓDICO	PÁGINA	FECHA	SECCIÓN
CRÓNICA	4	04/01/25	OPINIÓN

CÁMARA DE DIPUTADOS
LXVI LEGISLATURA
SOBERANÍA Y JUSTICIA SOCIAL

México es un país informáticamente vulnerable

Saúl Arellano
www.mexicosocial.org

La evolución del malware ha marcado un antes y un después en la seguridad informática global. Desde los primeros virus creados en los años 80 del siglo pasado, hasta las sofisticadas herramientas de ciberespionaje actuales, el panorama ha cambiado radicalmente. Hoy, los ataques informáticos son mayoritariamente impulsados por redes organizadas de ciberdelincuentes.

En la última década, el ransomware ha emergido como una de las principales amenazas. Este tipo de ataque cifra los datos de las víctimas y exige un pago, generalmente en criptomonedas, para su liberación. Ejemplos como WannaCry y NotPetya han demostrado el alcance devastador de estos ataques, que no distinguen entre empresas multinacionales, gobiernos o individuos. Además, la inteligencia artificial y el aprendizaje automático han dado lugar a nuevas formas de malware que se adaptan y evolucionan para evadir las medidas de seguridad tradicionales.

En México, las instituciones públicas han enfrentado serios retos en materia de ciberseguridad. La falta de inversión en tecnologías de protección y la vulnerabilidad de los sistemas obsoletos hace que muchas dependencias se encuentren expuestas a ataques.

Un caso emblemático es el de los Guacamaya Leaks, en el que un colectivo de hackers accedió a información confidencial de la Secretaría de la Defensa Nacional. Este incidente reveló la falta de prácticas de seguridad robustas, como la ausencia de encriptación en datos sensibles y sistemas sin actualizaciones.

Más recientemente, la Fiscalía de Nuevo León fue víctima de un ciberataque que paralizó sus sistemas y comprometió información clave sobre investigaciones en curso. De igual forma, gobiernos estatales y municipales han enfrentado secuestro de información mediante ransomware, lo que ha llevado a interrupciones de servicios esenciales, costos económicos elevados y pérdida de confianza ciudadana.

Por otra parte, instituciones financieras públicas como Nacional Financiera, el Banco del Bienestar y Banobras, desempeñan un papel crucial en la economía mexicana al facilitar recursos para proyectos de desarrollo y programas sociales. Sin embargo, estas instituciones son altamente atractivas para los ciberdelincuentes debido a los enormes volúmenes de dinero y datos sensibles que gestionan.

Entre los principales riesgos y amenazas para estas instituciones se encuentra el hecho de que los ciberdelincuentes buscan acceder a bases de datos de clientes y transacciones para realizar fraudes bancarios, suplantaciones de identidad o venta de información en mercados clandestinos.

Un ataque exitoso de los cibercriminales podría afectar no solo a individuos, sino también a empresas y proyectos gubernamentales de gran envergadura. Esto provocaría la interrupción de servicios financieros vía ataques de denegación de servicio (DDoS) que podrían paralizar sistemas de pago y transferencias, afectando desde el reparto de recursos sociales hasta la operación de grandes proyectos de infraestructura.

Otro tema crucial es la posibilidad de fraudes internos o accesos no autorizados. En efecto, los empleados con acceso a sistemas críticos pueden convertirse en vectores de ataque, ya sea por negligencia o colaboración con ciberdelincuentes. En el mismo nivel de riesgo estaría el Ransomware, un tipo de ataque ha afectado a instituciones financieras globales y representa una amenaza directa para bancos públicos. Los delincuentes secuestran sistemas y exigen rescates millonarios, comprometiendo la operación y la confianza pública. Un ejemplo relevante es el ocurrido en el 2018, cuando un ataque al Sistema de Pagos Electrónicos Interbancarios (SPEI) permitió el desvío de más de 300 millones de pesos.

Por su parte, el Poder Judicial, tanto en su nivel federal como estatal, enfrenta riesgos significativos en ciberseguridad debido a su manejo de información crítica relacionada con procesos legales, investigaciones y datos sensibles de ciudadanos y empresas. Por ejemplo, los ataques pueden comprometer investigaciones en curso, exponiendo a víctimas y testigos. Asimismo, la manipulación de datos puede llevar a la desaparición de evidencias, la alteración de fallos judiciales o el retraso intencionado de procesos legales.

> "Un caso emblemático es el de los Guacamaya Leaks, en el que un colectivo de hackers accedió a información confidencial de la Secretaría de la Defensa Nacional. Este incidente reveló la falta de prácticas de seguridad robustas, como la ausencia de encriptación en datos sensibles y sistemas sin actualizaciones"

Debe reconocerse que muchas dependencias judiciales operan con sistemas heredados que carecen de actualizaciones y parches de seguridad, lo que las convierte en blancos fáciles para ataques automatizados; lo que es más, en varias de ellas se opera con sistemas que no cuentan con licencias, como es el caso de varios juzgados familiares de la Ciudad de México.

Aunque hasta ahora no se conoce que la Suprema Corte de la Justicia de la Nación haya sido víctima de un ataque masivo, especialistas en ciberseguridad han señalado la necesidad urgente de modernizar sus sistemas para proteger información de alta relevancia nacional.

Al nivel de la población en general, la ciudadanía enfrenta riesgos significativos en el entorno digital. Entre los principales desafíos están: el robo o suplantación de identidad: Los ataques, las amenazas y la extorsión; y fraudes financieros, principalmente vía el mal uso de datos de tarjetas de crédito, débito y departamentales.

Por otro lado, los niños y niñas representan un sector especialmente vulnerable en el ámbito digital. Entre los riesgos más alarmantes se encuentran en primer lugar, el grooming, mediante el cual los depredadores aprovechan plataformas de redes sociales y videojuegos en línea para establecer contacto con menores, ganarse su confianza y, en casos extremos, explotarlos. En el mismo nivel está el Ciberacoso, la exposición a contenido inapropiado el robo de datos, y sobre todo, el enganche que se da para la explotación sexual comercial.

La seguridad informática en México enfrenta un panorama complejo, frente al cual una nueva cultura de la prevención es clave: invertir en infraestructura de seguridad, educar a la población y fomentar una cultura de ciberseguridad son pasos esenciales. Sin estas medidas, el costo de la ciberinseguridad seguirá aumentando.

Investigador del PUED-UNAM