Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD)

Tópico A: Medidas para enfrentar el *ransomware* como amenaza digital a la seguridad global

Introducción:

Además de atender distintas problemáticas en materia de drogas y justicia penal, la Oficina de las Naciones Unidas contra la Droga y el Delito tiene como mandato abordar de manera internacional diversos asuntos relacionados con la prevención del delito. Específicamente, la prevención de delito se entiende como "las estrategias y medidas encaminadas a reducir el riesgo de que se produzcan delitos y sus posibles efectos perjudiciales para las personas y la sociedad"[1].

A este respecto, el internet le ha otorgado una nueva dimensión al delito. En especial, destaca el tema relativo al *ransomware*, que se ha posicionado como una de las mayores amenazas para la ciberseguridad digital a nivel global. Básicamente, esta práctica consiste en cifrar archivos, permitiendo al ciberdelincuente obtener el control del sistema de una víctima y exigir un rescate económico a cambio de su liberación, lo que pone en riesgo la integridad y confidencialidad de la información.

En este sentido, la Organización de las Naciones Unidas actualmente reconoce el fraude, la manipulación de programas y datos de salida, las falsificaciones informáticas, el sabotaje, los virus, los gusanos y los *hackers* como una subdivisión de los delitos informáticos. Sin embargo, hacerle frente a este tipo de delitos requiere de recursos financieros y tecnológicos a los que no todos los países tienen acceso, lo cual ha mermado su capacidad de respuesta.

Por lo tanto, la cooperación internacional es esencial para fortalecer la seguridad digital y enfrentar eficazmente las amenazas actuales, garantizando así un entorno más resiliente y protegido contra posibles ciberataques. Para ello, es fundamental implementar diversas estrategias que aseguren de manera integral la protección de los distintos gobiernos, empresas, infraestructuras y servicios de consumo masivo.

Definición de conceptos:

- **Asociación de Examinadores de Fraude Certificados (ACFE):** organización internacional que reúne a más de 150 países para impulsar la prevención, detección y disuasión del fraude organizacional.

[1] Ver: Manual sobre la aplicación eficaz de las directrices para la prevención del delito (UNODC, 2010).

- ***Advanced Encryption Standard (AES)*:** algoritmo de cifrado de acceso público que está basado en una clave compartida.
- **Bomba lógica:** código oculto programable que cumple su acción maliciosa hasta cumplirse una serie de condiciones.
- ***Computer Emergency Response Team (CERT)*:** equipo de respuesta ante emergencias informáticas que se encarga de lidiar con incidentes en el marco de las redes de comunicaciones y sistemas informáticos.
- ***Cold-calling*:** proceso de mercadotecnia diseñado para atraer a posibles clientes o consumidores de un producto específico, sin que estas personas anticipen esa interacción.
- ***Cracker*:** persona que accede de forma no autorizada a sistemas informáticos con intenciones no éticas.
- ***Dropper*:** ejecutable que tiene la función de instalar un *malware* en el equipo en el que se ejecute.
- ***Honeypot*:** herramienta que se instala en una red o sistema informático que detecta ataques al servidor por parte de terceros, obteniendo información del ataque y del atacante.
- ***Informática forense*:** proceso de capturar, identificar, extraer y documentar una evidencia digital para su uso posterior en una demanda.
- ***Malware*:** software que sostiene el objetivo malicioso de dañar o infiltrar sin el conocimiento del propietario.
- ***Print-bombing*:** proceso mediante el cual los ciberdelincuentes acceden a las impresoras que se encuentran en la red de la víctima de *ransomware* para imprimir mensajes de rescate.
- ***Ransomware*:** *malware* que impide a los usuarios acceder a un sistema, o bien, a sus archivos personales y solicita un pago para poder ser "eliminado".
- ***Ransomware* como servicio (RaaS):** modelo de negocio que permite a los ciberdelincuentes alquilar herramientas de *ransomware*.
- **Tecnologías de la Información y la Comunicación (TICs):** conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, los cuales permiten la compilación, procesamiento, almacenamiento y transmisión de información.
- ***Uniform Resource Locator (URL)*:** dirección que identifica un contenido publicado en internet.

Problemática actual:

Uno de los mayores desafíos que representa el *ransomware* es que se ha transformado en un negocio lucrativo, en el que grupos criminales y delincuentes independientes operan desde el anonimato. Esto no sólo significa una amenaza a la seguridad de los sistemas informáticos, sino a la economía global, puesto que las pérdidas económicas derivadas de estos ataques son significativas, incluyendo el pago de rescates, los costos asociados a la recuperación de los datos y la disminución de la productividad por inactividad de las empresas atacadas.

De acuerdo con los datos del ESET Security Report, Latinoamérica ha sido una de las regiones mayormente afectadas por esta práctica, dado que en 2023 se registró un aumento considerable en cuanto a la cantidad de intentos para ejecutar ataques de *ransomware* contra sistemas corporativos y gubernamentales. El 96% de las organizaciones manifestó su preocupación y percibió al *ransomware* como una amenaza latente, mientras que el 21% reconoció haber sufrido un ataque mediante este tipo de *malware* en los dos años previos.

A su vez, el informe más reciente de ciberamenazas de Kaspersky también sostiene que las empresas latinoamericanas son las más afectadas por ataques de *ransomware*. Reportó que, en los últimos 12 meses, se alcanzaron a bloquear 1.15 millones de intentos de ataque en la región, siendo Brasil la zona más afectada con un total de 603 mil intentos de ataque, seguido por Ecuador con 212 mil y, posteriormente, México con 102 mil.[2]

Las vías más comunes para llevar a cabo esta práctica son las siguientes:

- Acceso a enlaces web o archivos adjuntos infectados.
- Conexiones directas al sistema de dispositivos externos infectados.
- Descarga de *softwares* de actualización falsos o infectados.
- Uso de criptomonedas.
- Visitas a páginas web comprometidas.

Así, la proliferación del *ransomware* no sólo ha impactado negativamente en la seguridad cibernética y la economía global, sino que ha generado un escenario propicio para la evolución de amenazas digitales más sofisticadas. Además de los canales comúnmente utilizados para llevar a cabo ataques de *ransomware*, es crucial explorar las tendencias emergentes que han surgido en este panorama dinámico.

Una de las preocupaciones crecientes, por ejemplo, es la convergencia del *ransomware* con el espionaje cibernético. Esta fusión de amenazas digitales ha permitido a actores malintencionados no sólo cifrar datos valiosos, sino también acceder y exfiltrar información confidencial antes de realizar el cifrado, aumentando la gravedad de los ataques. Este fenómeno ha llamado en mayor medida la atención de los expertos en ciberseguridad y

[2] *Empresas latinoamericanas reciben un promedio de dos ataques de ransomware por minuto, señala Kaspersky.* (2023, 30 agosto). Latam.kaspersky.com. https://latam.kaspersky.com/about/press-releases/2023_empresas-latinoamericanas-reciben-un-promedio-de-dos-ataques-de-ransomware-por-minuto-senala-kaspersky

gobiernos, dado que las implicaciones para la seguridad nacional y privacidad de los Estados son alarmantes.

En esencia, el *ransomware* mantiene su nivel de sofisticación en constante evolución. Se ha convertido en una industria criminal altamente lucrativa al punto en que han surgido sistemas de afiliados, en los que personas o colectivos colaboran con los creadores del *malware* para distribuirlo de manera personalizada. También se utilizan técnicas como el "*print-bombing*", que implica el uso de impresoras de la red de la víctima para imprimir mensajes de rescate, así como el "*cold-calling*", que involucra llamadas telefónicas que a veces culminan en extorsionar a la víctima.

Aunado a ello, en 2023, el panorama del *ransomware* reveló tendencias preocupantes. Los ciberdelincuentes comenzaron a utilizar Inteligencia Artificial (IA) para desarrollar códigos más elaborados y persuasivos. Además, surgió el modelo "*Ransomware* como servicio" (RaaS), el cual permite que delincuentes menos experimentados puedan llevar a cabo ataques sofisticados al alquilar o comprar kits completos de *ransomware* a otros actores maliciosos.

Especialistas como CS Lock, Eset, Kaspersky y Tanium destacan la importancia de implementar políticas de gestión de parches, realizar evaluaciones y gestión del riesgo de seguridad, aplicar controles de acceso y autenticación sólidos, implementar soluciones de seguridad y capacitar a los empleados en prácticas de seguridad cibernética. Adicionalmente, enfatizan la necesidad de realizar copias de seguridad para facilitar la recuperación de los datos en caso de un ataque.

De este modo, en términos generales, el combate contra el *ransomware* sigue siendo un desafío cada vez más complejo para los actores de la ciberseguridad, por lo que la colaboración entre canales, instituciones y expertos en seguridad cibernética es esencial para hacer frente a esta amenaza en expansión con la intención de proteger la integridad y confidencialidad de los datos en el entorno digital. En el ámbito internacional, la respuesta coordinada y la cooperación entre países se vuelven imperativas. A medida que los ciberdelincuentes operan sin fronteras, es esencial fortalecer los lazos entre las agencias de aplicación de la ley y las entidades gubernamentales para compartir inteligencia y coordinar esfuerzos destinados a identificar y procesar a los responsables.

El rol de las empresas y organizaciones en la prevención y mitigación de ataques de *ransomware* también es de suma importancia. Además de implementar medidas de seguridad avanzadas, la concientización y la capacitación de su personal son elementos clave en la defensa contra estos ataques. La colaboración entre el sector público y privado es imprescindible para enfrentar esta amenaza en constante cambio.

Iniciativas internacionales:

A nivel internacional y, en algunos casos, nacional, se han promovido alternativas de financiamiento para avanzar los esfuerzos de capacitación, asistencia técnica y mejores prácticas, así como procedimientos estandarizados para realizar informática forense y obtener evidencia digital válida, entre los cuales destacan los siguientes:

- Cooperar para realizar diligencias de investigación policial y obtener testimonios para los procesos judiciales, considerando también el uso de las TICs.
- Colaborar en la perturbación de los programas de secuestro de archivos mediante el intercambio de información, cuando sea apropiado y conforme a las disposiciones legales y reglamentarias aplicables.
- Combatir la capacidad de los perpetradores de programas de secuestro de archivos para obtener ganancias ilícitas mediante la implementación y el cumplimiento de medidas contra el lavado de dinero y la financiación del terrorismo.
- Elaborar guías, lineamientos y recomendaciones que impulsen la adopción de mejores prácticas y, de esta manera, ampliar el catálogo de capacitaciones enfocadas a distintos grupos interesados en combatir la cibercriminalidad (investigadores, fiscales, jueces, diplomáticos, legisladores).
- Establecer parámetros generales para el respeto y regulación de las políticas de privacidad sustentados en la homologación de estadísticas locales, regionales y globales.
- Fomentar la creación o fortalecimiento de CERTs en el sector financiero, académico, comercial y energético.
- Imponer responsabilidades a los perpetradores de programas de secuestro de archivos por sus acciones delictivas y negarles refugio seguro.
- Interrumpir y llevar ante la justicia a los perpetradores de programas de secuestro de archivos y a quienes lo facilitan, dentro de los límites permitidos por la legislación aplicable y las autoridades pertinentes.
- Promocionar entornos colaborativos con CERTs y empresas diversas de telecomunicaciones con tal de inferir la iniciativa privada que opera infraestructuras críticas de información o que está dentro de los sectores estratégicos, así como con empresas proveedoras de servicios gratuitos de internet, como correos electrónicos, mensajería instantánea, micro-blogs y servicios de transporte en línea.
- Recomendar un marco común mínimo en términos de protección de la información y transparencia para que, a pesar de las distintas políticas que cada Estado tiene a nivel nacional, se puedan compartir datos pertinentes sobre investigaciones y procesos judiciales.

A este respecto, desde 2021, Estados Unidos ha liderado formalmente la "Iniciativa Internacional de Lucha contra el *Ransomware*", a la cual se han sumado más de 40 países desde entonces. Estos Estados se comprometen a lo siguiente:

- Crear una lista negra compartida de monederos o direcciones de pago de rescates. Para lograrlo, se tienen contempladas dos plataformas de intercambio de información en las que los países miembros podrán aportar datos para identificar cómo los delincuentes reciben los pagos.
- No albergar delincuentes de *ransomware* dentro de sus territorios.
- No pagar los rescates. Esto de acuerdo con el argumento de Anne Neuberger, asesora adjunta de seguridad nacional de EEUU, quien asegura que mientras el dinero siga fluyendo hacia los delincuentes, el problema persistirá y empeorará.

Ahora bien, aunque se han implementado numerosas medidas a nivel internacional para abordar la problemática, aún se requiere el respaldo de las grandes potencias. La lucha se centra en destacar que la globalización del mundo digital constituye una amenaza de suma importancia, que no necesariamente involucra armamento convencional, sino invasiones e intromisiones que afectan la privacidad, entendida como un derecho y valor fundamental que atañe a los seres humanos.

Es crucial que la comunidad internacional en su conjunto reconozca que el entorno digital debe ser resguardado contra el comercio de información ilegal y otras extensiones perjudiciales para preservar la integridad de los derechos individuales. En ese sentido, la colaboración y coordinación a nivel global se tornan fundamentales para enfrentar eficazmente estos desafíos y garantizar un entorno digital seguro para las sociedades. Sin duda, el compromiso colectivo debe consistir en la puesta en marcha de iniciativas internacionales que incluyan la implementación de protocolos de seguridad robustos, la promulgación de leyes y regulaciones efectivas, y la participación de distintos actores en la detección y prevención de intrusiones digitales.

Preguntas guía:

1. ¿Su delegación ha experimentado ataques de *ransomware*? ¿Con qué frecuencia?
2. ¿Cuál es la magnitud de los ataques de *ransomware* que ha enfrentado su delegación y a qué sector suelen ser dirigidos?
3. ¿Cuáles han sido las acciones y políticas que ha implementado su delegación para hacerle frente a los ataques de *ransomware*?
4. ¿Cuáles son las sanciones establecidas en su delegación en lo que respecta a la comisión de ataques cibernéticos?
5. ¿Cuál es el tipo de apoyo o compensación que su delegación ofrece a las víctimas de estos ataques?
6. ¿Cuáles son las consecuencias que el *ransomware* ha generado en su delegación en los ámbitos político, económico y social, entre otros?

7. ¿Cuál es la inversión anual que su delegación realiza en beneficio de la ciberseguridad?
8. En su delegación, ¿qué medidas para combatir el *ransomware* han implementado los actores no gubernamentales?

Referencias bibliográficas:

- Bárbara Bécares. (2023, 2 noviembre). *España no negocia con hackers: se une a una iniciativa global para no pagar en los ataques de ransomware*. Genbeta. https://www.genbeta.com/actualidad/espana-no-negocia-hackers-se-une-a-iniciativa-global-para-no-pagar-ataques-ransomware
- Christopher Bayne. (2023). *La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)*. https://www.unov.org/unov/es/unodc.html
- *Empresas latinoamericanas reciben un promedio de dos ataques de ransomware por minuto, señala Kaspersky.* (2023, 30 agosto). Latam.kaspersky.com. https://latam.kaspersky.com/about/press-releases/2023_empresas-latinoamericanas-reciben-un-promedio-de-dos-ataques-de-ransomware-por-minuto-senala-kaspersky
- *Grupos de ransomware muy activos en América Latina en el 2023*. (2023). Welivesecurity.com. https://www.welivesecurity.com/es/cibercrimen/5-grupos-ransomware-activos-america-latina-2023/
- *Iniciativa Internacional de Contraprogramas de Ransomware:* refuerzo de la cooperación en materia de ciberseguridad. *(*2922, 3 noviembre). Unión Europea. https://digital-strategy.ec.europa.eu/es/news/international-counter-ransomware-initiative-strengthening-cybersecurity-cooperation-actions
- Poliveiraa. (2020). *Crime Prevention & Criminal Justice Module 2 Key Issues : 1-Definition of Crime Prevention*. https://www.unodc.org/e4j/es/crime-prevention-criminal-justice/module-2/key-issues/1--definition-of-crime-prevention.html
- Poliveiraa. (2020). *Crime Prevention & Criminal Justice Module 2 Key Issues : Summary*. https://www.unodc.org/e4j/es/crime-prevention-criminal-justice/module-2/key issues/summary.html
- Raúl Ortega. (2023, 31 julio). *Ciberdelincuencia simplificada 2023: el auge del ransomware como servicio (RaaS)*. eSemanal. https://esemanal.mx/2023/07/ciberdelincuencia-simplificada-2023-el-auge-del-ransomware-como-servicio-raas/
- Secretaría de Estado de Digitalización e Inteligencia Artificial. (s.f.). *Glosario de términos*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
- *Seguridad cibernética: un problema mundial que demanda un enfoque mundial*. (2022). Naciones Unidas. https://www.un.org/es/desa/seguridad-cibernetica