—LEGISLATURA—
H. CONGRESO DEL ESTADO DE AGUASCALIENTES

50 ANIVERSARIO
BENEMÉRITA
UNIVERSIDAD AUTÓNOMA
DE AGUASCALIENTES

ESTADO LIBRE Y SOBERANO
DE AGUASCALIENTES
PODER LEGISLATIVO

H. CONGRESO DEL ESTADO DE AGUASCALIENTES
SECRETARÍA GENERAL
RECIBIDO
15 JUN. 2023
RECIBE Ulises
FIRMA
HORA 10:36
PRESENTA Promovente
FOJAS 7

Aguascalientes, Ags., a 15 de junio del 2023.

HONORABLE SEXAGÉSIMA QUINTA LEGISLATURA
DEL H. CONGRESO DEL ESTADO DE AGUASCALIENTES
P R E S E N T E:

DIP. ANA LAURA GÓMEZ CALZADA Y DIP. JUAN LUIS JASSO HERNÁNDEZ, en nuestro carácter de integrantes de la LXV Legislatura del Honorable Congreso del Estado de Aguascalientes, con fundamento en lo dispuesto por los artículos 27, fracción I y 30, fracción I, de la Constitución Política del Estado de Aguascalientes; los artículos 16, fracciones III y IV, 108, 109, 112, y 114 de la Ley Orgánica del Poder Legislativo del Estado de Aguascalientes, y el artículo 153, fracción I, del Reglamento de la Ley Orgánica del Poder Legislativo del Estado de Aguascalientes, sometemos a consideración de esta Honorable Soberanía la **INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE ADICIONA LA FRACCIÓN III, AL ARTÍCULO 181 DEL CÓDIGO PENAL PARA EL ESTADO DE AGUASCALIENTES,** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

Los ciberataques en Latinoamérica aumentaron en 2022 y 2023 Así lo reveló la reciente edición del informe anual X-Force Threat Intelligence Index, elaborado por IBM Security.

De acuerdo con este reporte, aunque Latinoamérica representó el 12% de todos los ciberataques observados, la región pasó del quinto al cuarto lugar entre las regiones más afectadas del mundo. Según el reporte de IBM Security, Brasil, Colombia, México, Perú y Chile fueron los países latinoamericanos más atacados en 2022.

¿Y cuáles fueron los ataques más comunes en la región? El reporte señala que el líder indiscutible fue el ransomware, modalidad que concentró el 32% de los ataques. De hecho, el estudio señala que Latinoamérica fue la región que registró el mayor porcentaje en esta categoría a nivel global.

"El **Ransomware** es un tipo de malware que bloquea el dispositivo o cifra su contenido para extorsionar al propietario pidiéndole dinero. A cambio, los creadores de este código malicioso prometen -por supuesto, sin ningún tipo de garantías- restaurar el acceso al equipo infectado o a la información.

- ¿Qué es el ransomware?

Este tipo específico de software malicioso se usa para extorsionar. Cuando un dispositivo logra ser atacado con éxito, el malware **bloquea la pantalla o cifra la información almacenada en el disco** y se solicita un rescate a la víctima con los detalles para efectuar el pago.

- ¿Cómo reconocer el ransomware?

Si te han atacado, el ransomware te mostrará en la mayoría de casos **un mensaje de rescate** en la pantalla, o añadiendo un archivo de texto (mensaje) de las carpetas afectadas. Muchas familias de ransomware también **cambian la extensión de los archivos** cifrados.

- ¿Cómo funciona el ransomware?

Hay múltiples técnicas que los creadores de ransomware utilizan:

a) **Ransomware diskcoder:** cifra todo el disco y evita que el usuario acceda al sistema operativo.

b) **Screen locker:** bloquea el acceso a la pantalla del dispositivo.

c) **Crypto-ransomware:** cifra la información almacenada en el disco de la víctima.

d) **PIN locker:** ataca los dispositivos Android y cambia los códigos de acceso para dejar fuera a los usuarios."[1]

"El cibercrimen está sufriendo un importante cambio de paradigma. Durante los últimos años ha ido adquiriendo una naturaleza mucho más agresiva y generalizada, pero a la vez menos sofisticada. Además, la pandemia ha potenciado exponencialmente la criminalidad en internet.

La digitalización forzosa ha supuesto la aparición de factores de riesgo críticos para la ciberseguridad de ciudadanos, empresas e instituciones del Estado (especialmente para el sector educativo y sanitario).

La Europol ya ha advertido del surgimiento de una nueva categoría de cibercrímenes: los high tech crimes, unos ciberdelitos que se cometen utilizando *malware*, programas maliciosos que se infiltran y obtienen el control del sistema informático o del dispositivo móvil para robar información valiosa o dañar datos."[2]

"Crimen de alta tecnología es una forma de delito cibernético, el delito de alta tecnología se refiere a los delitos que utilizan tecnología electrónica y digital para atacar computadoras o una red informática.

Dichos delitos incluyen la piratería informática o cualquier uso o distribución no autorizados de datos, ataques de denegación de servicio y distribución de virus informáticos.

Los delincuentes de alta tecnología utilizan un conjunto de herramientas de malware,

[1] https://www.eset.com/es/caracteristicas/ransomware/
[2] https://www.eleconomista.com.mx/empresas/Sabotaje-ciberextorsion-o-estafa-El-reto-de-castigar-los-ciberataques-de-ransomware-como-delitos-20221013-0074.html

que van desde troyanos bancarios hasta ransomware y phishing, para organizar sus ataques."[3]

En nuestro País, la Guardia Nacional CERT-MX, indica que "Actualmente, los delincuentes utilizan técnicas más avanzadas de extorsión utilizando virus informáticos de tipo Ransomware, un programa que "secuestra" virtualmente la información de las víctimas al cifrar la información electrónica con un código que solo el delincuente cibernético conoce, para que la víctima entregue una recompensa a cambio del código de descifrado."[4]

"Palo Alto Networks, a través de su unidad especializada en inteligencia de amenazas Unit 42, dio a conocer los resultados de su *Ransomware Threat Report 2022,* que analiza el comportamiento de esta amenaza durante el último año.

El estudio posiciona a México como el segundo país de Latinoamérica en recibir el mayor número de ataques de ransomware, solo por detrás de Brasil. En concreto, Brasil recibió 39 incidentes reportados a Unit 42 y México 23; le siguieron Perú con 14, Argentina con 12 y Chile con 10. Cabe destacar que este número abarca solo los ataques reportados a la unidad de Palo Alto Networks, por lo que se estima que el número real puede estar por encima de esta cifra.
Cabe destacar además que el sector gobierno es el que más ataques con ronsmware registró en 2021 en México con por lo menos tres incidentes reportados por instituciones públicas.

El principal grupo criminal de ransomware que actúa en Latinoamérica es LockBit 2.0, un grupo cibercriminal que comenzó en 2019 y actualizó su programa de *Ransomware* en 2021.

Fue responsable de al menos 1 de 4 incidentes de Ransomware (23%) registrados en Latinoamérica y es también el grupo que encabezó los rankings por incidentes de ransomware en México con el 22%. El segundo más relevante es el grupo Prometheus, responsable del 19% de los ataques en Sudamérica.

El estado más atacado de México fue su capital, la Ciudad de México, con un total de 11 incidentes, seguida por San Luis Potosí, con tres y Michoacán, dos. Otras entidades con ataques registrados fueron Azcapotzalco, Cabo San Lucas, Guadalajara, Hidalgo, Jalisco y Quintana Roo, acumulando un total de 23 atentados en el país.

En cuanto a los ataques recibidos en México, el sector público fue el principal receptor de incidentes, con tres registrados, seguido de la industria de Materiales y los servicios al consumidor, con dos."[5]

"El ransomware ha sido uno de los ciberataques que más dolores de cabeza ha generado para diversas empresas (tanto pequeñas como grandes) en México y el mundo, y

[3] https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime/high-tech-crime
[4] https://www.gob.mx/gncertmx/articulos/ransomware
[5] https://clo.com.mx/mexico-segundo-pais-de-latinoamerica-que-recibe-mas-ataques-ransomware/

todo parece que lo seguirá haciendo por más tiempo.

De acuerdo con un reporte de la empresa de ciberseguridad Avast, los ataques de ransomware aumentaron 24% a nivel global durante el segundo trimestre del año. Para el caso de México, el riesgo de ransomware subió 14%.

Los mayores incrementos intertrimestrales en el ratio de riesgo de ransomware se produjeron en Argentina (+56%), Reino Unido (+55%), Brasil (+50%), Francia (+42%) e India (+37%).

Los consumidores, pero sobre todo las empresas, deben estar en guardia y preparados para los encuentros con el ransomware, ya que la amenaza no va a desaparecer pronto, explica Jakub Kroustek, director de investigación de malware de Avast.

Kroustek agrega que el descenso de estos ciberataques observado a finales de 2021 y principios de 2022 se debió a la captura del grupo de cibercriminales rusos Conti, especializado en ransomware; sin embargo, los miembros de la organización criminal se han ramificado para crear nuevos grupos de ransomware como Black Basta y Karakurt o unirse a otros como Hive, BlackCat o Quantum, provocando un repunte en la actividad de este tipo de ciberataque.

De hecho, un informe de Sophos de principios de año indicó que 74% de las empresas en México fueron víctimas de un ataque de ransomware durante 2021. Cada empresa mexicana afectada por uno de estos ciberataques pagó, en promedio, 482,446 dólares."[6]

"La actividad del ransomware en México creció 300 por ciento en los últimos meses, siendo el grupo LockBit responsable de la mayor parte de la ofensiva y los sectores gobierno y manufactura los más afectados.

Germán Patiño, vicepresidente de Ventas para Latinoamérica en Lumu Technologies, explicó que los investigadores de la empresa de ciberseguridad encontraron que LockBit realizó 32.8% de los ataques de ransomware registrados en México durante los dos últimos años, su víctima más reciente fue el Gobierno Municipal de Juárez.

Este grupo cibercriminal surgió a finales de 2019 y ha destacado por usar una variedad de técnicas que están poniendo en jaque a los equipos de ciberdefensa. Por ejemplo, técnicas antiforenses para sabotear las investigaciones; el borrado de servicios y puntos de recuperación; sus códigos maliciosos tienen la capacidad de autopropagación y pueden evadir y desactivar soluciones de protección.

Patiño resaltó que LockBit no es la única preocupación que deben tener las empresas y gobierno en México, ya que también han visto ataques provenientes de otros grupos como Conti y BlackCat."[7]

[6] https://businessinsider.mx/riesgo-ransomware-increment-14-por-ciento-mexico-segundo-trimestre-2022_tecnologia/
[7] https://www.excelsior.com.mx/hacker/crecieron-300-los-ataques-de-ransomware-en-mexico/1572358

"Tres de cada cuatro empresas mexicanas (74%) consultadas por Sophos fueron víctimas de ataques de ransomware en 2021. Los ciberdelincuentes lograron cifrar la información de sus víctimas en la mitad de los casos. Esto coloca a México como el país donde más empresas sufrieron un ataque de ransomware exitoso entre los mercados de América Latina analizados en el estudio El estado del ransomware 2022.

México está muy por encima de Brasil (55%), Colombia y Chile en cuanto al porcentaje de las empresas encuestadas que recibieron un ataque de ransomware durante el 2021 y, por tanto, está también por encima del promedio regional, que es de 66 por ciento. El incremento en el número de empresas atacadas es abrumador, pues en todos los países analizados se duplicó con respecto al 2020; mientras que en México se triplicó."[8]

"El aumento en el número de ataques de ransomware a empresas en México se ha triplicado en comparación con el año pasado, esta afectación no es únicamente para las empresas e instituciones de gobierno sino también para sus clientes y usuarios que usan estos servicios. Esta práctica de los hackers consiste en cifrar archivos vitales para la víctima y se exige una fuerte suma de dinero para recuperarlos y como resultado de que la mayoría de las empresas se encuentran en la web, sean grandes o start-ups, todas tienen un riesgo muy grande de ser atacadas por los ciberdelincuentes.

Se podría pensar que los casos ransomware solo suceden a las pequeñas empresas que no tienen suficiente capital para invertir en seguridad informática. A veces, si no se hace a través de servicios como **SAYNET**, puede representar una inversión significativa. Pero esto es falso; recientemente, cada vez más empresas como Canon, que se consideran grandes corporaciones globales, están siendo víctimas de ataques ransomware. ¿Por qué? Porque quieren ahorrar su capital en lugar de invertir en protegerse a sí mismos y a su información confidencial de los hackers, ignorando por completo un aspecto crucial de ser un negocio con presencia en línea.

En el caso de Canon, mundialmente conocido por sus impresoras y cámaras, la compañía fue atacada por el grupo ransomware identificado como Laberinto. En el informe escrito por Bleeping Computer (Abrams, 2020).

Canon confirmó en una nota interna que diez terabytes de su información fueron copiados, y como resultado, Maze amenazó a Canon para revelar estas toneladas de información copiada a menos que pagaran su rescate propuesto. Un experto en Fortinet (una de las alianzas estratégicas de SAYNET), comentó sobre el tema y expresó que los ataques ransomware son cada vez más actuales a medida que los ciberdelincuentes se están beneficiando de estas actividades maliciosas."[9]

"Enfocándonos al delito informático, el Dr. Julio Téllez Valdez, en su libro *Derecho Informático*, menciona el concepto típico de delitos informáticos: "*son las conductas típicas,*

[8] https://www.eleconomista.com.mx/tecnologia/Tres-de-cada-cuatro-empresas-mexicanas-fueron-victimas-de-ransomware-Sophos-20220511-0060.html
[9] https://saynet.com.mx/el-impacto-del-ransomware-en-mexico/

antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin"; y en el concepto atípico menciona que "*son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin*". Desde un punto particular, se podría definir al delito informático como "el acto u omisión que es realizado utilizando cualquier medio electrónico y que es sancionado por las leyes penales".

De las definiciones anteriores, se observa que el "acto" u "omisión" debe estar tipificado en una ley penal, si no lo está no podría considerarse como delito."[10]

Dos ejemplos de casos de ransomware, que por su alcance e intenciones queremos destacar: Yahoo y Sony.

- Yahoo

En 2013, fue víctima de un gran ataque informático que afectó a más de 1.000 datos personales de sus usuarios. Uno de sus grandes fallos fue, precisamente, haberse callado durante años, algo que provocó que su CEO fuera cesado de sus funciones.

La brecha de seguridad costó a Yahoo unos 3.000 millones de dólares, ya que se expusieron datos tan sensibles como direcciones de email, claves, cumpleaños, números de teléfono, nombres y apellidos de las personas registradas en la plataforma.

- Sony

En 2014, sufrió una serie de ciberataques a varias de sus divisiones que provocaron unas pérdidas millonarias a la compañía. Uno de esos ataques, mencionados por el propio Barack Obama como "un intento de extorsión", fue el que afectó al departamento audiovisual.

Concretamente, los cibercriminales se dedicaron a robar correos y películas de la compañía, provocando la cancelación de rodajes cinematográficos y, por ende, haciendo lo propio con los estrenos cinematográficos. Además de los ataques, se produjeron amenazas personales y, tras una larga investigación, el FBI responsabilizó de todos los incidentes a Corea del Norte.

Es importante que, como cualquier otra amenaza, la ciberseguridad se tome en serio, pues estos ataques han impactado en los negocios y personas de México y el mundo; pueden provocar una caída más allá de la económica en ciertos productos y servicios que son el blanco de ataque.

Por lo anteriormente expuesto, se propone el siguiente:

[10] https://revista.seguridad.unam.mx/numero26/delitos-inform-ticos-en-m-xico

PROYECTO DE DECRETO

ÚNICO. – Se adiciona la fracción III al artículo 181 del Código Penal para el Estado de Aguascalientes, para quedar de la siguiente manera:

ARTÍCULO 181.- Acceso informático indebido. El Acceso Informático Indebido consiste en:

I. Acceder a la información contenida en un aparato para el procesamiento de datos o cualquier dispositivo de almacenamiento de información sin autorización de su propietario o poseedor legítimo; o

II. Interferir el buen funcionamiento de un sistema operativo, programa de computadora, base de datos o cualquier archivo informático, sin autorización de su propietario o poseedor legítimo; **o**

III. Bloqueado el dispositivo o cifrando su contenido, sin autorización de su propietario o poseedor legítimo.

[...]

TRANSITORIOS

ÚNICO. - El presente Decreto iniciará su vigencia al día siguiente de su publicación en el Periódico Oficial del Estado de Aguascalientes.

ATENTAMENTE

DIP. ANA LAURA GÓMEZ CALZADA

DIP. JUAN LUIS JASSO HERNÁNDEZ

H. Congreso del Estado de Aguascalientes, **15 de junio del 2023.**