PERIÓDICO	PÁGINA	FECHA	SECCIÓN
La Razón	12	03/10/2022	COLUMNAS Y ARTÍCULOS

BAJO SOSPECHA

EL AHORRO EN CIBERSEGURIDAD SE PAGA CARO

POR BIBIANA BELSASSO

bibibelsasso@hotmail.c

Seis terabytes de información sensible fue robada de los servidores de la Secretaría de la Defensa Nacional (Sedena). Un grupo autollamado "Guacamaya" se adjudica el robo y ha hecho llegar los documentos a medios de comunicación y activistas. Estamos hablando de 36 millones de documentos PDF, 1.5 millones de fotos o tres mil horas de video.

Este caso ya es considerado el mayor robo cibernético de información en México. La información filtrada abarca del año 2016 a septiembre del 2022. Son datos confidenciales que no se habían querido dar a conocer, desde la salud del Presidente López Obrador hasta la forma en la que fue liberado Ovidio Guzmán, hijo de Joaquín *El Chapo* Guzmán en el llamado "Culiacanazo".

Esta información se difundió el pasado 29 de septiembre, y al día siguiente, el Presidente pareció restarle importancia y aseguró que era información que ya se conocía.

Pero lo más grave de todo esto es que *hackers* hayan obtenido información confidencial de esa manera. Y es que la seguridad cibernética es muy importante para proteger no sólo este tipo de información, sino hasta instalaciones estratégicas.

El 20 de febrero del 2022, la Auditoría Superior de la Federación advirtió en un documento de 38 páginas que había deficiencias en la administración y operación de 18 de los 20 controles de ciberseguridad para la infraestructura de *hardware* y *software* de la Secretaría de la Defensa.

Y es que si no se protege lo que hay en el ciberespacio, las consecuencias pueden ser gravísimas. Ahora fue robo de información, pero con sistemas computarizados como tenemos hoy en día, podrían tomar las torres de control de los aeropuertos, las instalaciones de gas o luz, entre otras.

Especialistas aseguran que, si hay una Tercera Guerra Mundial, ésta será cibernética. Lo vimos en mayo del 2021, cuando en Estados Unidos, un grupo de piratas cibernéticos cortó el flujo de petróleo del oleoducto más grande de ese país. Miles de personas se quedaron sin el servicio.

The Colonial Pipeline Company fue blanco de un ataque cibernético; cuatro ductos principales quedaron fuera de línea por varias horas, pero algunas terminales y puntos de entrega pequeños pudieron operar de forma parcial.

Colonial Pipeline transporta más de 100 millones de galones de combustible al día, a través de un oleoducto de productos refinados más grande de Estados Unidos, por donde traslada gasolina, combustible diésel y aceite para calefacción doméstica desde los estados de Houston, Texas, hasta el puerto de Nueva York.

De ataques cibernéticos se puede obtener información sensible para extorsionar u obtener millones de dólares mediante fraudes, lo hemos visto en empresas como Petróleos Mexicanos (Pemex) o ahora en la Sedena.

En 2020, platiqué con el especialista en seguridad cibernética, Marcos Rosales, nos habló de la importancia de mantener seguros nuestros dispositivos móviles y mantener actualizada la seguridad de los sistemas.

"Los sistemas operativos son como una casa, en la que para entrar hay 10 puertas, algunas van a tener cerraduras mucho más duras que otras, y las 2 actualizaciones lo que buscan es que, de esas 10 puertas que hay para entrar a una casa, todas tengan las llaves más seguras posibles para que cuando venga alguien a querer entrar no lo puede hacer, porque la chapa es supersegura, porque la puerta está básicamente blindada, entonces eso es lo que hacen estas actualizaciones por eso hay que mantener nuestros dispositivos actualizados y de ser posible con algunos sistemas como antivirus y seguridad en Internet", explicó.

HACKERS BUSCAN EXTORSIONAR A GOBIERNOS O EMPRESAS

Foto: Cuartoscuro

EN MÉXICO, Pemex, la Secretaría de Economía, la SFP, Condusef, entre otras dependencias, han sido blanco de un ataque cibernético.

La vulnerabilidad no sólo paraliza sistemas financieros, empresas o dependencias, actualmente muchos servicios están conectados a la red o a la nube, con lo que se podría llegar a perjudicar escuelas u hospitales al usar algún tipo *malware* de la familia del *ransomware* (en inglés significa secuestro de datos) para extorsionar a gobiernos o empresas.

Este tipo de ataques ya se consideran terrorismo. En entrevista, Luis Adrián Gómez, director de Cybolt, empresa especialista en ciberseguridad, me comentó que un *hackeo* a un aeropuerto puede generar consecuencias tan graves por ejemplo en el tráfico aéreo, que podría alcanzar catástrofes tan devastadoras como el ataque a las Torres Gemelas del 11 de septiembre de 2001.

"La forma de atacar, de hacer atentados ha evolucionado y es mucho más sencillo hacer ataques en los ámbitos digitales y mucho más eficiente. El gobierno estadounidense está haciendo alianzas con otras agencias de seguridad en otros países, para poder hacer una red, porque finalmente la forma de detener estos ataques es compartir información, si un ataque ocurre en algún lado y se comparte información a tiempo se puede evitar que ese ataque se reproduzca en otros países", subrayó.

En nuestro país hay otros casos de ataques cibernéticos. En noviembre de 2019, cuando se dio a conocer que Pemex fue blanco de un ataque cibernético con un *ransomware* del grupo DoppelPaymer, que exigió un pago por 565 bitcoins, unos cinco millones de dólares, a cambio de liberar los sistemas.

En febrero del 2020, la Secretaría de Economía detectó un ciberataque en algunos de sus servidores. Por esas fechas, también la Secretaría de la Función Pública (SFP) sufrió un *hackeo* al que se refirieron como "accidente de seguridad" y que expuso las declaraciones patrimoniales de 830 mil funcionarios públicos.

Entre el 5 y el 20 de julio de 2020 hubo ataques a la Condusef, a quien le quitaron el control completo de su web.

Los *hackeos* pueden ser tan peligrosos que pueden poner contra la pared a empresas transnacional o gobiernos poderosos. Basta recordar lo ocurrido en mayo de 2017 con la aparición del caso WannaCry.

Ese año, ordenadores de todo el mundo recibieron mensajes en los que se les avisó que sus documentos estaban cifrados y que sólo pagando un rescate en bitcoins podrían volver a tenerlos.

Más 300 mil equipos en más de 150 países sufrieron las consecuencias de la vulnerabilidad de Microsoft, conocida como EternalBlue y que afectaba a Windows, por lo que empresas que usaban ese sistema, perdieron 4 mil millones de dólares.

La importancia de tener una sólida ciberseguridad es fundamental para cualquier país. No se puede aplicar una política de austeridad en la protección a sistemas cibernéticos. Los costos de no hacerlo son altísimos.