Vulnerabilidades y cambios en algunos sectores

Incremento de los ataques cibernéticos en los últimos tres años.

Desde inicios de la pandemia ocasionada por el COVID-19

Los ciberdelincuentes no dudaron en sacar ventaja de los eventos sociales para incrementar los ataques de phishing, malware y ransomware.

Para 2020, el número de ataques cibernéticos a nivel global fue de 19.2 mil millones, lo que representa un incremento del 66% en comparación con el 2019[1], además el número de variantes de malware únicas aumentaron en un 128%, lo que evidencia la creciente sofisticación y complejidad de los mismos. El sector financiero, salud y educativo fueron los más afectados, con un incremento de 238% y 58% en ataques malware, y 30% en ataques ransomware respectivamente.

Durante el 2022, Colombia quedó como el segundo país en América Latina con mayor cantidad de ciber-ataques, y aunque los defensores lograron tener éxito a la hora de detectar y prevenir ransomware, los ciberdelincuentes han conseguido disminuir el tiempo promedio para completarlos, pasando de dos meses a menos de cuatro días[2]. Entre los tipos de ataques más comunes en Colombia se encuentran el phishing, la suplantación de identidad, el malware y los ataques de denegación de servicio (DDoS); además se ha evidenciado un incremento en los ataques de ransomware, en donde los ciberdelincuentes cifran los datos de la víctima para después exigir el rescate de su liberación.

En la actualidad, las organizaciones se enfrentan a una innovadora economía sumergida en la ciberdelin-cuencia, en donde las tácticas y los vectores de ataque al evolucionar casi minuto a minuto, amplían el panorama informático; más del 85% de los ciberataques son originados en el factor humano, lo que quiere decir que aunque los ciberdelincuentes utilicen una amplia gama de herramientas tecnológicas, la manipulación emocional sigue siendo el ingrediente principal a la hora de persuadir a sus víctimas.

Es por esto que debido al incremento de la ciberdelincuencia, tanto las empresas como las organi-zaciones gubernamentales han empezado a implementar las medidas adecuadas de ciberseguridad y cooperación entre los sectores públicos y privados; creación de programas de certificación en seguridad cibernética e incremento en la colaboración con los organismos internacionales para mejorar la seguri-dad a nivel global; lo que ha permitido contrarrestar los ataques y minimizar los riesgos para la seguridad humana.

1.Cyber threat report 2020 - SonicWall
2.X-Force Threat Intelligence Index - IBM®

Contenido

Mirada por sector

Las industrias y sus ciberriesgos

La adaptación de tecnologías emergentes como el Internet de las cosas (IoT), la inteligencia artificial (IA) y la nube, abre la posibilidad de que los ataques cibernéticos continúen aumentando en los próximos años, ya que los ciberdelincuentes siguen buscando formas de aprovechar las vulnerabilidades de los sistemas informáticos, mientras se especializan en los distintos sectores e industrias a los que se dirigen.

A continuación, daremos una mirada a determinados sectores con el propósito de ver a qué se enfrentan y qué medidas pueden utilizar para protegerse en el futuro.

Sector financiero

Un blanco con grandes brechas

El sector financiero es un amplio conjunto de entidades, instituciones y empresas que se dedican a actividades relacionadas con la gestión, el intercambio y la inversión del dinero.

En la actualidad, los ciberdelincuentes implementan nuevas técnicas para infiltrarse en los sistemas de las instituciones financieras, con el objetivo de obtener información valiosa que les permita llevar a cabo actos fraudulentos.

En el momento en el que las entidades de crédito y servicios financieros se empezaron a introducir en los procesos de pago en línea más rápidos e inteligentes y, a la vez, incrementaron el trabajo en casa de sus empleados, el número de ciberataques aumentó un 238%[3].

Una de las principales problemáticas actuales es el aumento de los ataques de ransomware, este tipo de malware bloquea el ingreso a los sistemas y datos de una empresa mientras accede a los datos sensibles de los clientes y los detalles bancarios personales, los cuales son vendidos o distribuidos por los atacantes, a menos de que la entidad afectada pague una gran suma de dinero por el rescate, esto no solo ocasiona una notable pérdida económica para la compañía sino que además su reputación y buen nombre quedan completamente afectados.

Dado que en este sector cualquier ataque permite convertir bits fraudulentos en dinero 'al portador', actualmente está enfrentando grandes retos en temas de sensibilización y capacitación en ciberseguridad para los empleados.

En particular si analizamos el ataque Petya y NotPetya, vemos como una ciberarma rusa dirigida contra objetivos en Ucrania, terminó causando estragos en el sector financiero colombiano.

Para hacer frente a estás problemáticas existen distintas alternativas que las organizaciones pueden utilizar. Una de ellas es el cifrado de datos, el cual consiste en transformar la información en un código que solo puede ser descifrado por las personas autorizadas, evitando la filtración en caso de un ataque. Además, la implementación de firewalls y antivirus actualizados, permite bloquear los intentos de infiltración de malware en los sistemas de la organización.

La criptografía, es una técnica de ciberseguridad que permite proteger la información mediante el uso de algoritmos codificados.

Estos alteran las representaciones codificadas en ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Al momento de querer implementar criptografía es importante identificar los datos críticos, seleccionar el algoritmo de cifrado adecuado, generar claves de cifrado seguras, proteger las claves de cifrado, implementar el cifrado de los sistemas y realizar pruebas de seguridad de manera regular; con una adecuada ejecución se logra proteger los datos financieros y garantizar la confidencialidad, integridad y disponibilidad de la información.

3.Financial services: Risk trends - Allianz® (2021)

Durante el 2022, se ejecutaron 566 violaciones de datos en el sector financiero. Dichos ataques dieron como resultado la exposición de más de 254 millones de registros.

El tipo de ataque más común fue la piratería general, la cual representó el 57% de todas las infracciones. El segundo fue el skimming, con 6,5% de las infracciones.

*The State of Data Breach Intelligence: 2022 Midyear Edition - Flashpoint

Sector salud

Ataques que quitan más que millones de dólares

El sector salud incluye una amplia gama de servicios y productos que abarcan desde la prevención y el diagnóstico hasta el tratamiento y la rehabilitación. La protección de los datos médicos y personales de los pacientes es fundamental para garantizar su privacidad y seguridad; sin embargo, debido a la gran cantidad de información personal y médica, los ciberdelincuentes han puesto el foco en dicho sector, lo que ha ocasionado el incremento de ataques cibernéticos en los últimos años.

Tanto la falta de conciencia e inversión en seguridad cibernética como el aumento de ataques en ransomware, son algunas de las problemáticas actuales por las que atraviesan.

Muchas organizaciones de salud no invierten suficientes recursos en seguridad cibernética, lo que las hace vulnerables a ataques de phishing, malware y otras técnicas de ciberdelincuencia.

Durante el 2017 un ataque conocido como NotPetya, el cual aparentaba ser un ransomware, logró destruir por completo los datos del software infectado, ocasionando daños aproximados de 10 mil millones de dólares, la farmacéutica multinacional Merck se responsabilizó de 870, y el excedente fueron asumidos por FedEx, Maersk, entre otras multinacionales.

Sin embargo, el robo, secuestro, pérdida de datos o pago de una gran cantidad de dinero; no son los únicos problemas que enfrenta el sector salud, sino que además se está viendo afectada la operación de los sistemas, ya que en el momento en el que la red informática es hackeada todo equipo que esté conectado a esta queda completamente deshabilitado, lo que impide que los pacientes puedan ser atendidos.

Es importante empezar a implementar medidas de protección, con el fin de salvaguardar los datos médicos y personales de los pacientes, como: crear y mantener los perfiles de red adecuados para los profesionales de la salud, incorporar autenticación multifactor, mantener una seguridad proactiva, realizar evaluaciones de diagnóstico cibernético avanzado para poder detectar las vulnerabilidades y corregirlas antes de que estas sean explotadas, implementar políticas de seguridad de datos, cifrado de datos e implementación de sistemas de monitoreo de seguridad.

Adicionalmente, tanto la capacitación del personal como la inversión en contratación de expertos en ciberseguridad, permitirá llevar a cabo soluciones efectivas y eficientes que reduzcan la superficie de ataque.

Sector educativo

Limitaciones presupuestales que incrementan vulnerabilidades

El sector educativo es un conjunto formado por las instituciones, organizaciones y empresas, que se dedican a la enseñanza y el aprendizaje en todas sus modalidades, abarcando desde la educación preescolar hasta la educación superior, sea profesional o técnica.

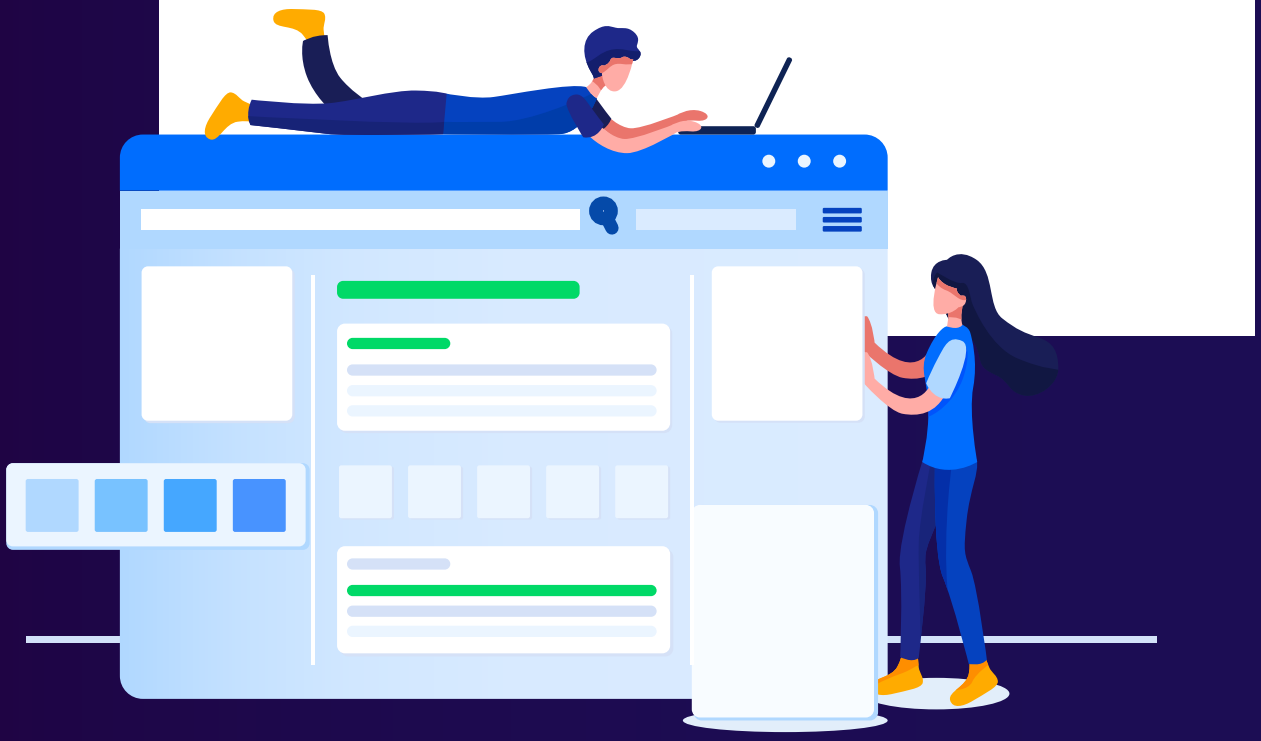
Con la llegada de la pandemia del COVID-19, la digitalización de documentos se empezó a acelerar, y con esto la necesidad de proteger los datos y el sistema educativo de posibles ataques cibernéticos; los hackers buscan extraer información personal, financiera y académica tanto de los estudiantes como del personal docente. Así mismo, el incremento de la educación en línea, y la falta de inversión en tecnología y ciberseguridad de algunas instituciones, ha dejado una extensa brecha para posibles ciberataques.

Entre 2020 y 2022, la educación y el área de investigación fueron unos de los principales objetivos de los ciberatacantes, teniendo un aumento del 114% y con una media de 2.000 ataques por organización cada semana durante dicho periodo[4]. El hecho de que incrementarán las organizaciones educativas en línea conllevó a ampliar el número de personas que no hacían parte del sistema educativo, las cuales lograban acceder a sus redes desde ubicaciones remotas, con gran exposición y elevando los riesgos de ser vulnerados.

Como ocurrió en el caso de Lincoln College, una institución universitaria que forma parte de la Universidad de Oxford. Dicha institución difundió un comunicado en mayo de 2022, en donde reportaba que después de 157 años activos, iban a suspender toda la programación académica al final del semestre de primavera; el motivo fue un ataque ransomware que impidió el acceso a los datos de reclutamiento, retención y recaudación de fondos para la institución; sumado a esto la pandemia ocasionó una crisis económica y junto con el ataque sufrido en diciembre de 2021, se frustraron los planes para fortalecer su posición financiera.

4.Cyber Attack Trends: 2022 Mid-Year Report - Check Point® Software Technologies Ltd.

Es necesario recalcar que la gran mayoría de ataques cibernéticos son ocasionados por el desconocimiento frente a la importancia de la ciberseguridad en cada uno de los sectores, es crucial que las organizaciones educativas implementen políticas de seguridad efectivas para proteger la información y los sistemas educativos, incluyendo la activación de firewalls, softwares antivirus, antispyware, y el cifrado de datos mediante el uso de algoritmos codificados. Por otra parte, la inversión en tecnología, ciberseguridad, actualización y mantenimiento de software, permitirá que sus sistemas logren detectar y prevenir intrusos mientras analizan de manera constante la seguridad de las redes.



Infraestructura crítica

Consecuencias dramáticas que paralizan

El sector de infraestructura crítica comprende de una amplia variedad de instalaciones, servicios y sistemas esenciales para el funcionamiento de la sociedad y la economía. Incluyendo los servicios relacionados con la energía, el agua, el saneamiento, el transporte, la comunicación, la salud, la seguridad pública, la defensa, entre otros.

A medida que los avances tecnológicos evolucionan a paso veloz, los sistemas críticos están cada vez más interconectados y automatizados, lo que conlleva a un incremento tanto en frecuencia como en complejidad y severidad de los ataques cibernéticos. En caso de que dichas infraestructuras fueran vulneradas, las consecuencias podrían ir desde la interrupción del suministro de energía hasta la caída de los sistemas de seguridad pública, logrando perjudicar la vida de los ciudadanos y la economía.

Como ocurrió en el 2021 con la petrolera Colonial Pipeline, quien sufrió un ataque de malware el cuál le obligó a cerrar su sistema, detener todas las operaciones del oleoducto e interrumpir el suministro de combustible, el 9 de mayo Joe Biden declaró estado de emergencia y dijo que este ataque fue lo que se cree el mayor ciberataque exitoso a la infraestructura petrolera en la historia de Estados Unidos.

No solo Estados Unidos sufrió las consecuencias de un ataque cibernético, sino también el Gobierno de Costa Rica en 2022, en el cual una ola de ataques de ransomware perjudicó a 27 instituciones públicas, incluyendo el Ministerio de Hacienda, el Instituto Meteorológico Nacional, el Ministerio de Trabajo y Seguridad Social, entre otros.

Dicho ataque ocasionó que el gobierno tuviera que dar de baja tanto a los sistemas informáticos utilizados para declarar impuestos, como los sistemas encargados del control y manejo de las importaciones y exportaciones, causando una pérdida de 30 millones de dólares estadounidenses por día. Fue tal la magnitud de dicho ataque que se tuvieron que declarar en emergencia nacional.

En definitiva, ningún sector está exento de atravesar una amenaza cibernética, y día a día estas siguen incrementando notablemente, es importante que las organizaciones empiecen a utilizar medidas de seguridad cibernética más avanzadas, las cuales les permitan detectar amenazas posibles antes de ser vulnerados; así mismo se espera que las regulaciones y los estándares de seguridad cibernética sean aún más estrictos para asegurar que aquellas organizaciones que operan en el sector de infraestructura crítica, puedan cumplir con los requisitos en cuanto a seguridad cibernética se habla.

cyte
We-know-how®

Estamos enfocados en desarrollar tecnología de punta desde Colombia para el mundo, permitiéndonos ser agentes de cambio de la seguridad cibernética, a través de la criptografía post-cuántica.

En cyte, nos proyectamos como referentes y pioneros a nivel nacional e internacional en la prestación de servicios de seguridad y protección de datos con tecnología criptográfica; logrando convertirnos en un aliado estratégico para las organizaciones.

Da clic y encuentra el producto ideal para tu organización.