MUNDO CP
CORPORATIVO PROFESIONAL

CORPORATIVO

CIBERSEGURIDAD EMPRESARIAL

La ciberseguridad es una preocupación real para las empresas de todos los tamaños y sectores. La creciente interconexión y dependencia de la tecnología ha abierto las puertas a una serie de amenazas cibernéticas, siendo el ransomware y el robo de información dos de las más graves y recurrentes. En este artículo, comentaremos con detalle estas amenazas, desde una perspectiva empresarial, e indicaremos cómo funcionan, las modalidades de ataque y las estrategias para mitigar sus impactos.

Por ello, la ciberseguridad empresarial se refiere a las prácticas, políticas y tecnologías implementadas por las organizaciones para proteger sus activos digitales, datos confidenciales y sistemas de información contra amenazas cibernéticas. La evolución constante de la tecnología y la sofisticación de los ataques han requerido que las empresas adopten un enfoque proactivo y multidimensional para garantizar su seguridad en línea.

Lo anterior, para contener ataques recurrentes, tales como el ransomware, que es un malware que cifra los datos y sistemas de una empresa, impidiendo su acceso, hasta que se pague un rescate a los ciberdelincuentes, que generalmente solicitan en criptomonedas. Este tipo de ataque puede tener un impacto devastador en las operaciones empresariales, causando interrupciones, pérdida de datos y daños a la reputación. ¿Te suena, que en quincena se caigan los sistemas bancarios?

El ransomware se propaga a menudo a través de correos electrónicos de phishing, o sitios web maliciosos. Una vez que el malware se infiltra en la red de la empresa, comienza a cifrar los archivos y mostrar mensajes de rescate. Los atacantes exigen un pago en criptomonedas para proporcionar la clave de descifrado y restaurar el acceso a los

datos, ya que bloquea el acceso a los archivos y sistemas hasta que se pague el rescate. En ese sentido, los ciberdelincuentes amenazan con filtrar los datos robados si no se paga el rescate

El ransomware es más frecuente de lo que podemos creer, por el valor de la Información empresarial, ya que la información es un activo invaluable para las empresas, desde datos de clientes hasta propiedad intelectual y estrategias comerciales. El robo de información puede causar daños financieros y legales significativos, así como perjuicio a la reputación.

Aunado a la modalidad anterior, existen otras modalidades de robo de información, como las siguientes:

1. Phishing. Los atacantes envían correos electrónicos falsos que parecen legítimos, con el objetivo de engañar a los destinatarios para que revelen información personal o financiera. Los enlaces en estos correos electrónicos a menudo conducen a sitios web fraudulentos que buscan robar información.

2. Spear Phishing. Similar al phishing, pero dirigido a individuos específicos o a grupos reducidos. Los atacantes investigan a fondo a las víctimas para personalizar los correos electrónicos y aumentar su tasa de éxito.

3. Whaling. Una forma avanzada de phishing que se dirige a altos ejecutivos y líderes dentro de una organización. Los atacantes buscan acceder a información financiera o estratégica sensible.

4. Pharming. Los atacantes manipulan las configuraciones de dominios de Internet, o redirigen el tráfico web para redirigir a las víctimas a sitios web maliciosos sin su conocimiento, lo que permite el robo de información.

5. Keylogging. Los keyloggers registran las pulsaciones de teclas de las víctimas, lo que les permite robar contraseñas, números de tarjetas de crédito y otra información confidencial.

6. RATs (Remote Access Trojans). Son programas maliciosos que se instalan en las computadoras de las víctimas y permiten a los atacantes tomar el control remoto del sistema, acceder a archivos y robar información.

7. ¬Malware de robo de datos. Estos programas maliciosos están diseñados específicamente para robar información sensible almacenada en sistemas informáticos. Pueden extraer contraseñas, archivos y otros datos confidenciales.

8. Ingeniería social. Los atacantes manipulan psicológicamente a las víctimas para que revelen información sensible o realicen acciones no deseadas. Esto puede incluir llamadas telefónicas, interacción en redes sociales y manipulación emocional (muy común en México).

9. Ataques de fuerza bruta. Los atacantes intentan todas las combinaciones posibles de contraseñas hasta encontrar la correcta para acceder a cuentas o sistemas.

10. Fugas internas. Los colaboradores, ya sea de manera voluntaria o involuntaria, pueden filtrar información confidencial, ya sea por negligencia o intención maliciosa.

11. Ataques a la cadena de suministro. Los atacantes se infiltran en los proveedores de una organización para acceder a sus sistemas y, posteriormente, robar información confidencial de la organización.

12. Ataques de ingeniería inversa. Los delincuentes descomponen productos o software para acceder a su código fuente, lo que puede revelar información sensible o vulnerabilidades.

13. Intercepción de datos. Los atacantes interceptan comunicaciones en línea, como correos electrónicos o transacciones financieras, para robar información confidencial.

14. Skimming. Los agresores instalan dispositivos físicos en cajeros automáticos o puntos de venta para robar información de tarjetas de crédito o débito.

15. Ataques Man-in-the-Middle (MitM). Los atacantes se interponen en la comunicación entre dos partes legítimas para interceptar y robar información transmitida.

16. Ataques a dispositivos Internet de las cosas. Los dispositivos de Internet de las cosas mal protegidas, pueden ser explotados para robar información o acceder a redes corporativas.

17. Ataques de redes Wi-Fi públicas. Los atacantes pueden establecer redes Wi-Fi falsas en lugares públicos para interceptar el tráfico y robar información de los usuarios.

18. Ataques a redes sociales. Los ciberdelincuentes pueden utilizar perfiles falsos o técnicas de ingeniería social para robar información personal de las redes sociales.

La proliferación de ataques de ransomware y robos de información en los últimos años ha dejado en claro que ninguna empresa está exenta de ser objeto de ciberataques. Los ataques no solo pueden causar interrupciones operativas significativas, sino que también pueden tener un impacto a largo plazo en la reputación de la empresa, la confianza del cliente y la viabilidad financiera; Por tanto, la inversión en ciberseguridad y la adopción de mejores prácticas de protección de datos son imperativas para asegurar un futuro digital sólido.

La prevención es el primer paso crítico en la lucha contra las amenazas cibernéticas. La educación y la concienciación de los colaboradores son esenciales para crear una cultura de seguridad sólida dentro de la organización. Los colaboradores deben comprender los riesgos asociados con el phishing, la ingeniería social y otras tácticas utilizadas por los ciberdelincuentes para robar información confidencial. Al proporcionar capacitación regular y pruebas de phishing simulado, las empresas pueden mejorar la capacidad de detección y reducir el riesgo de caer en trampas digitales.

La implementación de soluciones de seguridad avanzadas también desempeña un papel fundamental en la protección de los activos digitales. Los firewalls, las soluciones antivirus, la detección de intrusos y el cifrado de datos son herramientas esenciales para mantener a raya a los ciberdelincuentes. La actualización

constante de software y sistemas es igualmente crucial para cerrar posibles vulnerabilidades que los atacantes puedan explotar. Además, la gestión de identidad y acceso (IAM) permite controlar quién puede acceder a qué información, reduciendo los puntos de acceso potenciales para los ciberdelincuentes.

La planificación de la respuesta a incidentes es otro componente vital en la estrategia de ciberseguridad empresarial. Las organizaciones deben establecer un plan claro y detallado que aborde cómo responder en caso de un ataque cibernético. Esto incluye identificar roles y responsabilidades, establecer líneas de comunicación claras y definir los pasos para mitigar el impacto del ataque y recuperarse de él. Cuanto más preparada esté una empresa para manejar un ataque, menos daño potencial podrá causar.

La colaboración también juega un papel crucial en la ciberseguridad empresarial. Las organizaciones deben trabajar en conjunto con socios externos, como proveedores de servicios de seguridad, agencias gubernamentales y otros actores de la industria, para compartir información sobre amenazas y mejores prácticas. La colaboración puede ayudar a anticipar y contrarrestar las tácticas de los ciberdelincuentes de manera más efectiva.

En última instancia, la ciberseguridad empresarial es un esfuerzo continuo que requiere vigilancia continua y adaptación a un panorama en constante cambio. Las amenazas cibernéticas evolucionan rápidamente y se vuelven cada vez más sofisticadas, lo que significa que las empresas deben estar preparadas para enfrentar nuevos desafíos en cualquier momento. La inversión en ciberseguridad no es solo una necesidad, sino una inversión estratégica en la sostenibilidad y el crecimiento de la empresa en el mundo digital actual.

Licenciado Diego Cárdenas Aguilar
diegocardenas@despachocardenas.com
www.despachocardenas.com
.