Octubre/2023 EDICIÓN Nº 10

BOLETÍN INFORMATIVO

THOR LTDA
SEGURIDAD PRIVADA

Clientes y proveedores

¿QUÉ ES LA CIBER SEGURIDAD?

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionara los usuarios o los usuarios o interrumpir la continuidad del negocio

BENEFICIOS DE LA CIBER SEGURIDAD EN LAS ORGANIZACIONES

- **Mayor seguridad de los datosMejor control de acceso**
- **Protección de la infraestructura de red**
- **Cumplimiento de los requisitos legales**
- **Confianza de los clientes**
- **Mayor productividad del equipo**
- **Control del riesgo de pérdidas financieras**

¿CUÁLES SON LOS CIBERATAQUES MÁS COMUNES?

El ransomware: Se caracteriza por restringir el acceso a un sistema informático y pedir un rescate para eliminar el bloqueo.

Este tipo de ciberataque puede ser fatal para una compañía porque implica una pérdida masiva de datos, además de perjuicios económicos

Ataque de denegación de servicio o DDoS: Entre los ataques más comunes y peligrosos está el DDoS o dedenegación del servicio, que consiste en provocar la caída de un servidor sobrecargando su ancho debanda. Estas acciones fuerzan la interrupción de unsitio web

Troyanos bancarios: Los troyanos pueden instalarse en cualquier dispositivo por visitar un sitio web infectado, por descargar el anexo de un mail, o incluso, por bajar una aplicación. Una vez este virus se instale en elcelular, detecta en qué momento se utilizan los servicios en línea de un banco y así capturar los datos personales y bancarios.

¿CÓMO PREVENIR ATAQUES INFORMÁTICOS?

Evita amenazas a través de emails: Los correos electrónicos son uno de los puntos más débiles de una compañía, pues a través de estos se pueden introducir de forma fácil amenazas de virus y robo de información, sin embargo, muchas empresas creen que no son tan peligrosos e ignoran la actividad de los correos internos y pueden ser víctimas de secuestro de datos.

Detecta a tiempo códigos maliciosos: Es común que estos códigos se escondan en archivos PDF, Html, GIF y Zip. Una buena práctica que no debes dejar de lado, es escoger un antivirus que pueda descubrir, decodificar y descifrar estos códigos ocultos y así evitar ser víctima de robo de información.

Reconoce las conexiones sospechosas: Frecuentemente,los cibercriminales usan direcciones IP, sitios web, archivosy servidores de correo electrónico con un histórico deactividad maliciosa

Monitorea las bases de datos: La modificación de la estructura en el banco de datos e intentos no autorizados de acceso a datos críticos pueden ser una señal de alerta que indica que la red estaría amenazada, para prevenir esto, usa herramientas que te ayuden a monitorear bases de datos y a registrar intentos de acceso no autorizado.

En **Thor LTDA,** cada día nos comprometemos con una misión vital y salvaguardar la seguridad de la información en todos los niveles de la organización y fortalecer las defensas, anticipar desafíos y garantizar la integridad de los datos.

NUESTROS CERTIFICADOS

icontec ISO 9001
CO-SC-CER600142

icontec ISO 14001
CO-SC-CER887124

icontec ISO 45001
CO-ST-CER887125

BASC
BUSINESS ALLIANCE FOR SECURE COMMERCE
COLBOG00924-1-3