Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | #2 | Prevención de Fuentes y Ataque e Intrusión

Seguridad Informática 1

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Rodríguez

ALUMNO: Pilar Barajas Cervantes

FECHA: 11/09/2024

índice

Introducción

El futuro de la seguridad informática está en la cooperación internacional, donde el trabajar el análisis de riesgo se vuelve impredecible. La seguridad informática es un tema para la protección y gestión de la información de cualquier información, por lo que es de suma importancia reconocer las categorías que existen para determinar las acciones en cada una de ellas. La seguridad informática completa cuatro áreas principales.

- **Confidencialidad: solo usuarios autorizados pueden acceder a recursos, datos e información.**
- **Integridad: solo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.**
- **Disponibilidad: los datos deben ser disponibles para los usuarios cuando sea necesario.**
- **Autenticación: verifica que realmente se están comunicando con quien se está comunicando, de acuerdo. De acuerdo a los elementos de objeto de protección clasificamos estos tipos de seguridad informática.**
- **Seguridad de hardware**
- **Seguridad de software.**
- **Seguridad de red.**

Descripción

Realizar copias de seguridad de los archivos periódicamente ayudara a cualquier empresa a no ser victima de los ciberdelincuentes una de las mejores opciones para proteger a las empresas de los virus informáticos es instalar un antivirus, aun que debemos saber que el propio sistema tiene mecanismo para autoprotegerse. Hay que tener especial precaución con las redes sociales nunca se puede abrir un archivo sin comprobar su origen. Siempre serrar el sitio web cuando el navegador indique que no es un sitio seguro. Tener un software de protección es el primer paso, mantenerlo es el segundo. Un software antivirus gratuito es mejor que nada, peso se debe de tener en cuenta que no es la mejor solución. Microsoft proporciona un paquete de seguridad gratuito, ya que, si se tiene Windows en el equipo, se le concede acceso.

La seguridad informática, también conocida como ciberseguridad es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existe una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura a la información. La ciberseguridad comprende software, (base de datos, metadatos, archivos) hardware, redes de computadoras y todo lo que la organización entienda.

Justificación

Con la transformación digital, las organizaciones han quedado más expuestas a los ataques informáticos. Debido a que los cibercriminales operan de manera encubierta y no son fáciles de detectar, pueden pasar mucho tiempo antes de que los problemas sean visibles para la organización. aunque algunas amenazas pueden ser detectadas, la gran mayoría pasara desapercibida. Por eso una detección temprana siempre será necesaria. Puede parecer obvio, pero ignorar la actividad de los correos internos es una falla común en todas las empresas. Los correos electrónicos son uno de los puntos más débiles de una organización, pues a través de ello se pueden detectar fácilmente las amenazas. Monitorear la actividad de mensajes sospechosos, así como la descarga de archivos anexos. Estar alerta al tráfico anormal, de la red protocolos, aplicaciones o actividad de los usuarios. Se debe presentar atención al volumen del tráfico y los cambios inesperados en el uso del protocolo.

Al identificar los códigos maliciosos los malware y los códigos generalmente se esconden en formatos comunes de archivos. (PDF, HTML, GIF, ZIP etc.) una buena práctica consiste en escoger un antivirus capaz de descubrir, decodificar y descifrar estos códigos ocultos. Los cibercriminales a menudo usan direcciones IP, sitios web archivos y servidores de correo electrónico con un histórico de actividad maliciosa utilizan herramientas capaces de examinar la reputación de fuentes no confiables ubicadas fuera de la organización.

Tabla de recomendaciones

Amenaza/ Vulnerabilidad+D14:I18	Amenazas Humanas	Amenazas Lógicas	Amenazas Fisicas	Vulnerabilidades de Almacenamiento	Vulnerabilidade de Comunicación
Factor de Riesgo	Contraseñas y usuarios basicas ficil de utilizar por cualquier persona	Desconociemiento del software utilizado.	Firewall inhavilitado, esto puede hacer que la redsea más vulnerable a un acceso no autorizado.	Equipos lentos sin espacio de almacenamiento.	No contar con el uso del equipo para las actividades de negado, por ejemplo el acceso a redes sociales o al manejo de correo electronico.
Recondaciones	Generar contraseñas diferentes en cada equipo de trabajo y realizar el cambio en periodos constantes esto evitara las funetes de ataque e intrusión.	todo personal que trabaja, en la ingenieria tiene que tener la información del software utilizado ya que esto evitará a no caer en las amenazas logicas del mundo cibernetico.	realizar la configuración del firewall, esto puede ayudar a que se bloqueen las nuevas amenazas o los nuevos tipos de tráfico comercial.	Revisar el material de los equipos de ptotecciònpara asegurar su perfecto estado y optimo funcionamiento	Contar con un contror del equipo de trabajo y evitar ingresar a ligas no confiables.
Fuente de Ataque e intrusión	Los ciberneticos prodrian recurrir a los fallos de seguridad con contraseñas facil de adivinar.	Los atacantes pueden utilizar la fuente de ataque utilizando caballos de Troya ya que con el desconocimiento del software que se esta utilizando estos podrian aprobecharse con programas que se hacen pasar por programas validos.	Los ciberneticos pueden recurrir a los dispositivos que no tienen configuradas las opciones de seguridad y aprobecharse de las vulnerables a los ataques.	Los atacantes pueden recurrir a los ataques de Malware y así pueden afectar la seguridad y la infrastructura de almacenamiento de los datos	Los atacantes pueden recurrir al Phishing y hacerse pasar por entidades confiables para obtener la información confiable.

Conclusión

En conclusión, la implementación de la detección de amenazas y respuesta a incidentes las 24 x hora de día, los 7 días de la semana ayuda a reducir el alcance de los impactos de un ciberataque exitoso. La organización se enfrenta a una amplia gama de ciberamenazas potenciales, incluyendo PHISHIN, MALWARE Y ATAQUE DoS. Las soluciones de detección y prevención de amenazas son esenciales para identificar y bloquear el contenido y el tráfico malicioso antes de que llegue a su destino previsto, monitoreo continuo. Los ciberataques son una amenaza continua, es probable que una empresa no solo sea el objetivo durante el horario comercial estándar. La ciberdelincuencia es una preocupación seria para cualquier empresa, y la gestión de estas amenazas es esencial para el éxito de la empresa. Algunas de las mejores prácticas que las organizaciones pueden implementar para reducir el riesgo de ciberataques.

La ciberseguridad se ha convertido en una de las principales preocupaciones de muchas empresas. Un ciberataque exitoso puede ser dañino y costoso, por lo que invertir en ciberseguridad es la opción lógica. Al poner en marcha las herramientas, los procesos y las soluciones adecuadas, una organización puede reducir drásticamente el riesgo potencial y el impacto de un incidente de ciberseguridad. Sin embargo, una estrategia de ciberseguridad esta alineada a los objetivos empresariales de la empresa y se basa en el conocimiento de las amenazas a al que es probable que se enfrente una organización.

Referencia

Check Point Software. (2024, 11 septiembre). Check Point Software: Leader in Cyber Security Solutions. https://www.checkpoint.com/

Pirani: We make risk management simple. (s. f.-b). Pirani. https://www.piranirisk.com/

Santander Corporate website. (s. f.). Santander Bank. https://www.santander.com/