Piedecuestana
DE SERVICIOS PÚBLICOS e.s.p.

Área de Sistemas de Informática

Riesgos Cibernéticos





RANSOMWARE



DESCRIPCIÓN

Consiste en el bloqueo, por parte de un hacker, de un dispositivo electrónico y en la encriptación de los archivos para que el usuario dueño no pueda acceder a la información y datos almacenados.



OBJETIVO

Presionar a las víctimas para que paguen un rescate que les devuelva el acceso a su información o sistemas.



IMPACTO

Hacer pública información privada sobre una persona o entidad con el propósito de ampliar el poder intimidatorio del ataque y forzar el pago.



PREVENCIÓN

1. Asegúrese de que el firmware, las aplicaciones anti-malware, los sistemas operativos y los softwares de terceros tienen instalada la revisión más reciente.
2. La capacitación y sensibilización de los usuarios reduce enormemente el riesgo de infección.
3. Las copias de seguridad evitan la demanda del rescate al recuperar los datos desde otra fuente que no sean los archivos cifrado.



PHISHING

DESCRIPCIÓN

Consiste en correos electrónicos o mensajes de texto que aparentemente son enviados por fuentes confiables y que persuaden al destinatario a completar una acción, abrir un enlace malicioso, que va poner en riesgo la información personal o de la empresa.

OBJETIVO

Compartir contraseñas, números de tarjeta de crédito, y otra información confidencial haciéndose pasar por una institución de confianza en un mensaje de correo electrónico o llamada telefónica.

IMPACTO

En promedio, un ataque de suplantación de identidad, exitoso le cuesta a una organización 1,6 millones de dólares estadounidenses, lo cual es un gran éxito sólo porque alguien ha hecho clic en un enlace o ha abierto un archivo adjunto.

PREVENCIÓN

1. Aprende a identificar claramente los correos electrónicos sospechosos de ser phishing.
2. Verifica la fuente de información de tus correos entrantes.
3. Nunca entres en la web de tu banco pulsando en links incluidos en correos electrónicos.
4. Refuerza la seguridad de tu ordenador.



SPEAR PHISHING

DESCRIPCIÓN

Obtener datos de valor dirigiéndose a una persona o empresa específica luego de haberse ganado su confianza. Este ataque es muy utilizado con empresas y personas reconocidas.

OBJETIVO

Divulgación de información confidencial por parte de los empleados de forma accidental. Empleados con malas intenciones y sin escrúpulos que ponen en riesgo la información de la empresa.

IMPACTO

El 30% de los correos electrónicos de phishing son abiertos por el destinatario previsto, y el 12% de los destinatarios hacen clic en un enlace malicioso o abren un archivo adjunto malicioso desde un correo electrónico de phishing. Como resultado, se estima que el 95% de los ataques cibernéticos exitosos dirigidos a empresas empiezan como un correo electrónico de phishing submarino.

PREVENCIÓN

1. Introduce tus datos confidenciales únicamente en webs seguras.
2. Revisa periódicamente tus cuentas.
3. Ante la mínima duda se prudente y no te arriesgues.



MALWARE

DESCRIPCIÓN

Obtener datos de valor dirigiéndose a una persona o empresa específica luego de haberse ganado su confianza. Este ataque es muy utilizado con empresas y personas reconocidas.

OBJETIVO

Divulgación de información confidencial por parte de los empleados de forma accidental. Empleados con malas intenciones y sin escrúpulos que ponen en riesgo la información de la empresa.

IMPACTO

El 30% de los correos electrónicos de phishing son abiertos por el destinatario previsto, y el 12% de los destinatarios hacen clic en un enlace malicioso o abren un archivo adjunto malicioso desde un correo electrónico de phishing. Como resultado, se estima que el 95% de los ataques cibernéticos exitosos dirigidos a empresas empiezan como un correo electrónico de phishing submarino.

PREVENCIÓN

1. Introduce tus datos confidenciales únicamente en webs seguras.
2. Revisa periódicamente tus cuentas.
3. Ante la mínima duda se prudente y no te arriesgues.



INYECCIÓN SQL

DESCRIPCIÓN

Es un ataque a la web que consiste en la infiltración de un código malicioso que aprovecha errores y vulnerabilidades de una página web. Es utilizado para robar bases de datos, manipular o destruir información.

OBJETIVO

Los hackers recurren a los ataques de inyección de SQL con el fin de introducirse en la base de datos de un sitio web. A veces solo quieren eliminar datos para provocar el caos y, en otras ocasiones, lo que buscan es editar la base de datos, especialmente en el caso de sitios web financieros.

IMPACTO

Eliminar datos para provocar el caos y, en otras ocasiones, lo que se busca es editar la base de datos, especialmente en el caso de sitios web financieros.

PREVENCIÓN

1. No proporcione información personal en sitios web sospechosos. Al introducir datos confidenciales, asegúrese de hacerlo solo en sitios web de confianza.
2. Manténgase informado de las noticias sobre los sitios web que utiliza y, si ve algo en referencia a una SQLI, cambie sus credenciales de inicio de sesión.
3. Acostúmbrese a crear contraseñas seguras.



ATAQUE DDOS

DESCRIPCIÓN

El ataque DDoS envía varias solicitudes al recurso web atacado, con la intención de desbordar la capacidad del sitio web para administrar varias solicitudes y de evitar que este funcione correctamente.

OBJETIVO

- Sitios de compra por Internet.
- Casinos en línea.
- Cualquier empresa u organización que dependa de la prestación de servicios en línea.

IMPACTO

Inhabilitar un servidor, un servicio o una infraestructura mediante el envío de un gran número de peticiones.

PREVENCIÓN

- Restringir el tráfico directo de Internet a ciertas partes de nuestra infraestructura, como los servidores de bases de datos. En otros casos, utilizar firewalls o listas de control de acceso (ACLs).
- Para mitigar ataques DDoS volumétricos de gran escala se debe tener en cuenta y analizar la capacidad del ancho de banda (o tránsito) y la capacidad del servidor de absorber.



SPAM

DESCRIPCIÓN

Es el equivalente electrónico del "correo basura" que pasa por debajo de tu puerta o llega a tu buzón. Sin embargo, el spam es más que algo molesto.

(Tomado de: https://latam.kaspersky.com/)

OBJETIVO

- Ganar dinero con el pequeño porcentaje de destinatarios que acaba respondiendo al mensaje.
- Ejecutar estafas mediante prácticas de phishing, con el objetivo, entre otras cosas.

IMPACTO

1. El spam bloquea los canales de comunicación y crea tráfico que debe ser pagado por el proveedor.
2. Si el spam llega a la bandeja de entrada, el destinatario tiene que eliminarlo manualmente.
3. Perder un correo electrónico importante por tener que eliminar una gran cantidad de correo no deseado.

PREVENCIÓN

1. Los proveedores más populares de correo electrónico ofrecen un botón útil para poder denunciar un mensaje como spam.
2. No haga clic en enlaces, no descargue archivos adjuntos y nunca responda a los spammers.
3. No publique su información de contacto.
4. Mantenga actualizado el software del sitio web para protegerse de los spammers que tratan de aprovechar vulnerabilidades.



SPYWARE

DESCRIPCIÓN

Puede supervisar y copiar todo lo que escribe, carga, descarga y almacena. Algunas cepas de spyware también son capaces de activar cámaras y micrófonos para verlo y escucharlo sin que usted se dé cuenta.

OBJETIVO

- Keylogging (registrar todo lo que escribe, etc.).
- Grabar audio y video, o realizar capturas de pantalla.
- Controlar el dispositivo de forma remota.
- Capturar contenido de las aplicaciones.
- Registrar y capturar su historial de navegación.

IMPACTO

Consumir una gran cantidad de recursos del ordenador, lo que provoca que se ejecute lentamente, retrasos entre aplicaciones o mientras está online, fallos o bloqueos frecuentes del sistema e incluso una sobrecarga del ordenador que causa daños permanentes.

PREVENCIÓN

1. Sea selectivo con lo que descarga en su equipo. Asegúrese de necesitar realmente un programa antes de descargarlo.
2. Lea los contratos de licencia.
3. Tenga cuidado con los avisos publicitarios interactivos.
4. Trate de evitar los programas (especialmente los programas gratuitos) que emiten avisos publicitarios interactivos.



WHALING

DESCRIPCIÓN

O “caza de ballenas” están dirigidos a perfiles directivos como CFO’s o CFO’s y otros cargos altos de las organizaciones con el objetivo de robarles información confidencial a la que ellos tienen acceso.

OBJETIVO

- Método que usan los cibercriminales para atacar directamente a los altos ejecutivos u otras personas importantes dentro de una organización, con el objeto de robar dinero o información.

IMPACTO

Este tipo de ataque también es conocido como fraude CEO, ya que el whaling se vale de técnicas de suplantación de identidad de sitios web y direcciones de correo electrónico para engañar a sus objetivos y hacer que revelen información confidencial de la empresa o hacerles transferir dinero a una cuenta.

PREVENCIÓN

1. Las organizacionee deben educar tanto a su personal como a los altos ejecutivos para identificar y prevenir las amenazas a la seguridad cibernética de la empresa.
2. Consulta directamente al remitente antes de tomar medidas.
3. La adopción de protocolos de seguridad de correo electrónico es la mejor vía para el incremento de la seguridad en todas las empresas sin importar su tamaño.



APPS MALICIOSAS

DESCRIPCIÓN

Son app poco fiable que acaba por infectar nuestro dispositivo, tomar control y robar la información que tenemos almacenada en él como contactos, credenciales, imágenes, videos, etc.

OBJETIVO

- Espiar el móvil.
- Robo de credenciales bancarias.
- Descargar un gusano informático para propagarse a través de nuestra lista de contactos, o hacerse con el control remoto del terminal.
- Grabar la pantalla del móvil y usar cámaras.

IMPACTO

Infectar el dispositivo móvil con algún tipo de malware que se camuflan como aplicaciones legítimas ocasionando robo y pérdida de información.

PREVENCIÓN

1. Debemos tener en cuenta utilizar tiendas oficiales. Además, debemos revisar las valoraciones y comentarios de otros usuarios e información del desarrollador. Al instalarla, nos pedirá aceptar una serie de permisos, que no debemos dar a no ser que esté relacionada con la función de la app.



Piedecuestana
DE SERVICIOS PÚBLICOS e.s.p.

OFICINA

Sistemas E Informática

Empresa Municipal de Servicios Públicos
Domiciliarios de Piedecuesta E.S.P.

jsistemas@piedecuestanaesp.gov.co