¿QUE ES LA SEGURIDAD DE LA RED?

Para CONECTA COMUNICACIONES es importante que tu navegación en internet sea una experiencia placentera y segura, es por ello que a continuación te informamos algunos conceptos y pautas para que puedas usar nuestro servicio de manera segura.

Conceptos básicos de seguridad de red

Métodos de seguridad de red
Para implementar este tipo de defensa en profundidad, hay una variedad de técnicas especializadas y tipos de seguridad de red.

Control de acceso: debe poder bloquear a usuarios y dispositivos no autorizados de su red. Los usuarios que tienen acceso autorizado a Internet solo han sido autorizados para utilizar el sitio web.

Antimalware: virus, gusanos y troyanos por definición de una red, y puede permanecer inactivo en las máquinas infectadas durante días o semanas. Su esfuerzo de seguridad debe hacerse para prevenir infecciones y también para el malware raíz que se dirige a su red.

Seguridad de la aplicación: su red suele acceder a las aplicaciones no seguras. Debe usar hardware, software y procesos de seguridad para bloquear esas aplicaciones.

Análisis de comportamiento: debe saber cómo es el comportamiento normal de la red para poder detectar anomalías o infracciones a medida que ocurren.

Prevención de pérdida de datos: los seres humanos son inevitablemente el enlace de seguridad más débil. Debe implementar tecnologías y procesos para garantizar que los empleados no envíen deliberadamente o inadvertidamente datos confidenciales fuera de la red.

Seguridad del correo electrónico: el phishing es una de las formas más comunes de obtener acceso a una red. Las herramientas de seguridad de correo electrónico pueden bloquear tanto los mensajes entrantes como los salientes con datos confidenciales.

Firewalls: quizás el abuelo del mundo de la seguridad de la red, siguen las reglas de su red o de Internet, estableciendo una barrera entre su zona de confianza y el salvaje oeste. No excluyen la necesidad de una estrategia de defensa en profundidad, pero siguen siendo imprescindibles.

Detección y prevención de intrusos: estos sistemas escanean el tráfico de red para identificar y bloquear ataques.

Movíl y seguridad inalámbrica: los dispositivos inalámbricos tienen todos los posibles fallos de seguridad de cualquier otro dispositivo conectado en red. Se puede conectar a casi cualquier red inalámbrica en cualquier lugar, lo que requiere la seguridad extra.

Segmentación de red: la segmentación definida por software en diferentes clasificaciones y facilita la aplicación de políticas de seguridad.

Información de seguridad y gestión de eventos (SIEM): estos productos pretenden reunir información de una variedad de herramientas de red para proporcionar los datos que necesita para identificar y responder a las amenazas.

VPN: Una herramienta (típicamente basado en IPsec o SSL) que autentica la comunicación entre un dispositivo y una red segura, creando un "túnel" seguro y encriptado a través de la Internet abierta.

Seguridad web: debe poder controlar el uso del personal interno para bloquear amenazas basadas en la web del uso de navegadores como vector para infectar su red.

Tipos De Amenazas En La Red

MALWARE: es un código o software malicioso que tiene el propósito de afectar, dañar o deshabilitar los sistemas informáticos y otorga un control limitado o total de los sistemas al creador del malware con el propósito de robo o fraude.

Tipos de Malware

- **Troyanos**: Se presentan al usuario como un programa aparentemente legítimo, pero que al ejecutarlo, le brinda al atacante acceso remoto al equipo infectado.
- **Backdoor**: Son puertas traseras donde el hacker pueda mantener el acceso al sistema sin que el usuario pueda notarlo.

- **Ransomware**: Permite bloquear un dispositivo desde una ubicación remota y encriptar archivos quitando el acceso a la información y datos almacenados.
- **Gusanos**: Puede replicarse a sí mismo en los equipos o a través de redes de computadores sin que te des cuenta de que el equipo está infectado.
- **Spyware**: Recopila información de un equipo y después transmite esa información a una entidad externa sin el consentimiento del propietario de la información.
- **Botnet**: Es una red de equipos que han sido infectados por malware y se ejecutan de manera autónoma y automática.
- **Crypter**: Tipo de software que puede encriptar y manipular malware, para que sea más difícil de detectar mediante programas de seguridad.
- **Virus**: Software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático.
- **Phishing:** es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.
- **Spam:** correo basura, correo no deseado o correo no solicitado hacen referencia a los mensajes de correo electrónico no solicitados, no deseados o con remitente no conocido.
- **Pharming:** es un tipo de ciberataque con el que se intenta redirigir el tráfico web al sitio del atacante, explotando vulnerabilidades de software en los sistemas de nombre de dominio o en los equipos de los propios usuarios, que permiten a atacantes redirigir un nombre de dominio a otra máquina distinta.

Contramedidas para el Malware

- Instalar un software antivirus
- Generar una política de antivirus
- Mantener actualizado el software de antivirus
- Evitar abrir archivos adjuntos de remitentes desconocidos
- Mantener con regularidad Backups de la información
- Programar escaneos regulares para todos los dispositivos
- No abrir dispositivos o programas sin analizarlos por el antivirus
- No utilizar software pirata.

Recomendaciones de Seguridad

Pornografía Infantil

Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

Control de virus y códigos maliciosos

Mantenga siempre un antivirus actualizado en su equipo(s), procure correr éste periódicamente, de la misma manera, tenga en su equipo elementos como anti-spyware y bloqueadores de pop-up (ventanas emergentes).

Evite visitar páginas no confiables o instalar software de dudosa procedencia. La mayoría de las aplicaciones peer-to-peer contiene programas espías que se instalan sin usted darse cuenta.

Asegúrese que se aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.

Si sus programas o el trabajo que realiza en su computador no requieren de pop-up, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas, deshabilite estos.

Si así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

Correo electrónico:

- No publique su cuenta de correo en sitios no confiables.
- No preste su cuenta de correo ya que cualquier acción será su responsabilidad.
- No divulgue información confidencial o personal a través del correo.
- Si un usuario recibe un correo con una advertencia sobre su cuenta bancaria, no debe contestarlo
- Nunca responda a un correo HTML con formularios embebidos
- Si ingresa la clave en un sitio no confiable, procure cambiarla en forma inmediata para su seguridad y en cumplimiento del deber de diligencia que le asiste como titular de la misma.

Control de Spam y Hoax:

- Nunca hacer click en enlaces dentro del correo electrónico aun si parecen legítimos. Digite directamente la URL del sitio en una nueva ventana del browser
- Para los sitios que indican ser seguros, revise su certificado SSL.
- No reenvié los correos cadenas, esto evita congestiones en las redes y el correo, además el robo de información contenidos en los encabezados.

Control de la Ingeniería social:

- No divulgue información confidencial suya o de las personas que lo rodean.
- No hable con personas extrañas de asuntos laborales o personales que puedan comprometer información.
- Utilice los canales de comunicación adecuados para divulgar la información.

Control de phishing y sus modalidades:

- Si un usuario recibe un correo, llamada o mensaje de texto con una advertencia sobre su cuenta bancaria, no debe contestarlo.
- Para los sitios que indican ser seguros, revise su certificado SSL.
- Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.

Robo de contraseñas:

- Cambie sus contraseñas frecuentemente, mínimo cada 30 días.
- Use contraseñas fuertes: Fácil de recordar y difícil de adivinar.
- Evite fijar contraseñas muy pequeñas, se recomienda que sea mínimo de una longitud de 10 caracteres, combinada con números y caracteres especiales.
- No envié información de claves a través del correo u otro medio que no esté encriptado.

Nuestros Mecanismos de Seguridad

En CONECTA COMUNICACIONES contamos con diferentes mecanismos de seguridad que ayudan a garantizar la seguridad en la red. Algunos de estos mecanismos son:

Firewall: A través de este elemento de red se hace la primera protección perimetral en las redes de CONECTA COMUNICACIONES y nuestros usuarios, creando el primer control que reduce el nivel de impacto ante los riesgos de seguridad.

Antivirus: Tanto las estaciones de trabajo como los servidores de procesamiento interno de información están protegidos a través de sistemas anti códigos maliciosos.

Antispam: Todos los nuestros servidores de correo poseen antispam que reduce el nivel de correo basura o no solicitado hacia los clientes, descongestionando los buzones y el tráfico en la red.

Filtrado de URLs: para el bloqueo de sitios con contenido de pornografía infantil, hemos fortalecido el filtrado de estos sitios a través de nuestros proveedores de internet. El objetivo principal de este filtrado es denegar el acceso a los sitios que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales. Se sugiere instalar además sistemas parentales.

Seguridad a nivel del CPE: Los dispositivos de conexión final ubicados en las premisas de los clientes cuentan con elementos bases para la autenticación y autorización, con ello permiten hacer una conexión a Internet de manera más segura.