IMPLEMENTACIÓN DE SISTEMAS INTERNOS DE SEGURIDAD EN LA RED

En cumplimiento a lo establecido en la Resolución CRC 5050 de 2016, EMTEL S.A E.S.P. publica en su página web los procedimientos técnicos para garantizar la seguridad en la red y la integridad del servicio, tales como el uso de firewalls, filtros antivirus y la prevención de spam, phishing, malware entre otras.

Frente a las acciones tomadas en relación al servicio prestado a sus usuarios de acceso a internet en banda ancha, EMTEL S.A. ESP cuenta a la fecha con los siguientes sistemas:

1. Para los usuarios del servicio de banda ancha, que requieren cuentas de correo con el dominio de emtel.net.co, se cuenta con un sistema de protección Antispam/Antivirus para el software de correo, los cuales previenen la perdida de información y garantizan la integridad de la información almacenada en sus cuentas de correo suministrada por EMTEL S.A. E.S.P.

2. Frente a la Autenticación de los usuarios del servicio de acceso a internet, EMTEL S.A. E.S.P, dispone de plataformas y procesos, que permiten en tiempo real, asegurar la autorización de acceso a la navegación vía la verificación de identidad (información residente en el equipo lado usuario – CPE) del usuario que intenta conectarse. Lo anterior asegura que solo usuarios autorizados puedan hacer uso de los servicios contratados con la compañía.

3. La plataforma en operación de EMTEL S.A. E.S.P, cuenta con funcionalidades de Accounting (Servicio de no repudio), esto es, que genera logs para cada una de las sesiones de usuario, donde se relaciona una dirección IP dinámica con la cuenta única asociada para cada cliente (asegura la identidad), fecha de inicio y duración de la sesión. Estos datos son almacenados mes a mes y guardados por un periodo de máximo un (1) año.

4. Frente a la Confidencialidad de los datos EMTEL S.A. E.S.P, dispone de sistemas que almacenan la información (almacenamiento masivo de datos) con protecciones que evitan la intrusión indebida a éstos. A su vez frente a los datos biográficos de sus usuarios, tiene establecidos procesos que garantizan la recepción y trámite de los requerimientos allegados solo desde los entes de seguridad mediante los cuales, se realiza la solicitud de información confidencial asociada a los usuarios de línea básica y datos (Ej. direcciones IP). Dicha solicitud debe estar soportada mediante orden judicial.

5. Complementando lo anteriormente expresado, y específicamente en lo que compete al principio de Integridad de datos, EMTEL S.A. E.S.P cuenta con mecanismos de protección del CORE de la Red, como son: Firewalls y filtrado perimetral, lo cual evita y elimina el riesgo de acceso no autorizado a la data correspondiente al servicio de correo de sus usuarios. Actualmente por disposición legal, se filtran las páginas de pornografía infantil publicadas por el ministerio de Comunicaciones Ley 679 (Esto se hace a través de los URL reportados en la página).

SOLUCIÓN FIREWALL

EMTEL S.A. E.S.P para proteger la granja de servidores y aplicaciones destinadas a la prestación de los diferentes servicios, así como su red interna de operación, de los flujos de entrada frente a ataques, o el acceso no autorizado a sus servidores y aplicaciones, posee un esquema de seguridad perimetral basado en una plataforma FORTINET que permite filtrar tráfico no deseado hacia la red

Esta plataforma de seguridad, permite la protección del acceso no autorizado y evitar intrusos en la red, y permite el establecimiento de políticas de acceso, hacia los diferentes servidores y aplicaciones de administración y control de los servicios de los usuarios, además de la base de datos de los usuarios autorizados. Mediante mensajes de alerta de esta plataforma, permite monitorear procesos de intrusión a las redes internas, aplicaciones o servicios protegidos por el Firewall.

RIESGOS RELATIVOS AL SERVICIO DE INTERNET

Internet se ha convertido en un servicio por medio del cual los usuarios realizan muchas de sus cosas cotidianas, es por esta razón que se debe ser muy consciente que esta tecnología trae consigo riesgos que pueden afectar la seguridad y privacidad, es así que EMTEL, informa a sus usuarios sobre estos riesgos y da algunas recomendaciones para tener en cuenta; Dentro de los riesgos se tienen:

Malware: "Malware" es una forma abreviada del término inglés "malicious software" (software malicioso) y hace referencia a virus, spyware, gusanos, etc. El malware está diseñado para causar daños a equipos independientes o conectados en red. Siempre que oiga esta palabra, piense en cualquier programa diseñado para dañar su equipo, ya sea un virus, un gusano o un troyano.

Virus: Son programas diseñados para infiltrarse en su ordenador y dañar o alterar sus archivos y datos. Los virus tienen la capacidad de corromper o eliminar los datos de su equipo. Y al igual que los virus naturales, también se replican. Un virus informático es más peligroso de que un gusano informático, ya que modifica o elimina sus archivos, mientras que los gusanos solo se replican sin efectuar cambios en sus archivos o datos.

Spyware: Programa espía que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Scam: es una palabra de origen inglés, cuya traducción es timo o estafa, su significado lleva a una historia o situación, en la que se dice que uno o varios individuos entregan una cantidad de dinero al estafador o “Scamer” con la promesa de recibir a cambio un beneficio generalmente económico (algún tipo de premio).

Phishing: es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

Ciberacoso: (derivado del término en inglés cyberbullying) también denominado acoso virtual o acoso cibernético, es el uso de medios de comunicación digitales para acosar a una persona o grupo de personas, mediante ataques personales, divulgación de información confidencial o falsa entre otros medios. Es decir, se considera ciberacoso, o ciberagresión a todo

aquello que se realice a través de los dispositivos electrónicos de comunicación con el fin intencionado de dañar o agredir a una persona o a un grupo.

Grooming: es una práctica de acoso y abuso sexual en contra de niños y jóvenes que, en la mayoría de los casos, sucede a través de las redes sociales. Afortunadamente, evitar que esto suceda es muy fácil, basta con tomar medidas de prevención y seguridad de navegación en Internet.

Robo de información: se produce cuando una persona adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de efectuar o vincularlo con algún fraude u otro delito.

En relación con la prevención de fraudes por suplantación de identidad, EMTEL S.A E.S.P realiza verificación y control, así:

- Para servicios se debe solicitar fotocopia de la cédula ampliada al 150% y huella.
- Se valida previamente la información antes de la instalación de los servicios.

POR PARTE DEL USUARIO

Como parte de la responsabilidad en el manejo del servicio de internet en sus equipos terminales se hacen las siguientes recomendaciones:

- Instalar herramientas antivirus.
- Para servicios bancarios tratar de utilizar siempre el mismo dispositivo, preferiblemente cableado al modem, es decir sin conexión wifi y menos si son públicas.
- Las contraseñas que use que tengan al menos ochos caracteres alfanuméricos.
- Cerrar siempre la sesión cuando se haya autenticado con usuario y contraseña, Así evita robo de información personal.
- No publicar datos personales en redes sociales. Y mantener privados los perfiles para que solo accedan las personas que usted autorice.
- No abrir los correos o noticias falsas, casi siempre estos se utilizan para robar información a través de software malicioso.

En los siguientes enlaces, puede leer más sobre las amenazas para la seguridad de la red:

https://socialtic.org/blog/8-buenas-practicas-de-seguridad-digital-para-todo/
https://www.guiainfantil.com/articulos/educacion/nuevas-tecnologias/internet-y-las-redes-sociales-riesgos-para-los-ninos/

CONTROL PARENTAL

Como su propio nombre indica, el control parental es una característica especialmente útil para padres y responsables educativos que desean impedir que niños o adolescentes puedan acceder a páginas Web inapropiadas. Además, gracias al filtro personalizado que incluye, también se puede

utilizar el control parental para impedir que otros tipos de usuarios puedan acceder a páginas Web con los contenidos que se especifiquen.

Este tipo de control le permite establecer límites para los siguientes casos:

Límites de tiempo. Puede establecer límites temporales para controlar el momento en que los niños pueden iniciar una sesión en el equipo. Los límites de tiempo impiden que los niños inicien una sesión durante las horas especificadas. Puede establecer distintas horas de inicio de sesión para cada día de la semana. Si hay una sesión iniciada cuando finalice el tiempo asignado, se cerrará automáticamente.

Juegos. Puede controlar el acceso a los juegos, elegir una clasificación por edades, elegir los tipos de contenido que desea bloquear y decidir si desea permitir o bloquear juegos específicos o sin clasificar

Permitir o bloquear programas específicos. Puede impedir que los niños ejecuten determinados programas.

El usuario administrador de Windows es el que puede aplicar filtros al resto de usuarios del PC, siempre que éstos no sean también administradores. Es decir, un usuario administrador puede aplicar filtros al resto de usuarios de Windows (usuarios estándar o restringidos), de modo que éstos sólo puedan acceder al tipo de páginas que el administrador haya establecido. Esto significa que deberán existir varios usuarios creados en Windows.

Para crear cuentas de usuario en Windows o modificar las existentes, haga clic en **Inicio** > **Panel de control** > **Cuentas de usuario**. Si necesita más información sobre las cuentas de usuario de Windows, consulta la ayuda de su sistema operativo.

Configure el control parental en su equipo Windows 10, siguiendo estos pasos:

Paso 1: Haga clic en el botón Inicio y seleccione Configuración.
Paso 2: En el menú de configuración, seleccione la opción Cuentas.
Paso 3: En la parte izquierda de la pestaña, seleccione Familia y otros usuarios. Verá que en la parte derecha de la pantalla aparecen las cuentas vinculadas a su equipo. Desde allí puede agregar más cuentas o configurar las que ya tiene.
Paso 4: Haga clic en la opción Administrar la configuración de la familia en línea.
Paso 5: Se abrirá una página de internet donde verá las cuentas vinculadas. Haga clic sobre las opciones de la cuenta que quiere configurar.
Paso 6: Configura los controles parentales como desee. Puede modificar la exploración web del menor, solicitar informes por correo electrónico de las actividades que realice, limitar o bloquear aplicaciones, juegos no adecuados para su edad, definir el tiempo que el niño puede usar el dispositivo, controlar las compras que se hagan en la tienda Windows y ver la ubicación de él.

En el siguiente enlace, puede ver un tutorial de cómo habilitar el servicio de control parental:

https://www.youtube.com/watch?v=iYFTaKN9Rmk