MECANISMOS DE SEGURIDAD EN LA RED

En cumplimiento de la resolución 3067 de 2011, Articulo 2.3 de seguridad en la red, INGEMTEL SAS dispone de los siguientes mecanismos para garantizar la seguridad en la red y las comunicaciones con respecto a los siguientes puntos:

1. Autenticación: Verificación de identidad tanto de usuarios, dispositivos, servicios y aplicaciones. Lainformación utilizada para la identificación, la autenticación y la autorización debe estar protegida (Recomendaciones UIT X.805 y UIT X.811).
Para el cumplimiento, INGEMTEL SAS tiene implementadas plataformas de autenticación de equipos terminales mediante la validación de la direcciones MAC (Media Access Control) y listas de direcciones IP fija asignadas por el personal técnico correspondiente, además dispone de procesos y políticas de seguridad mediante contraseñas y direcciones IP autorizadas para el acceso conocido únicamente por el personal técnico encargado para evitar la violación y alteración de los datos en los equipos terminales y en los equipos de transporte de la red.

2. Acceso: Prevenir la utilización no autorizada de un recurso. El control de acceso debe garantizar que sólo los usuarios o los dispositivos autorizados puedan acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones (Recomendaciones UIT X.805 y UIT X.812).
Para que cada equipo terminal tenga Acceso a la red debe ser registrado en al menos 2 equipos que hacen parte la red CORE en los filtros de listas de acceso, quienes autentican el dispositivo en cuestión y permiten su paso por la red de INGEMTEL SAS.

3. Servicio de No repudio: Es aquél que tiene como objeto recolectar, mantener, poner a disposición y validar evidencia irrefutable sobre la identidad de los remitentes y destinatarios de transferencias de datos. (Recomendaciones UIT X.805 y X.813).
Los mecanismos y sistemas de autenticación, además de los equipos generan Logs para cada usuario, donde se puede evidenciar información como direcciones IP asociadas a cada usuario, hora y fecha de conexión, además de graficas de consumo, disponible para ser consultada por el equipo técnico encargado en caso de evidenciar una anomalía o violación en el acceso a la red.

4. Principio de Confidencialidad de datos: Proteger y garantizar que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados (Recomendaciones UIT X.805 y X.814).
Con el fin de asegurar que la información de los usuarios no se pondrá a disposición de entidades o personas no autorizadas, INGEMTEL SAS tiene definido una política de tratamiento de la información de los usuarios Habeas Data, que garantiza que la información no será compartida bajo ninguna circunstancia, a excepción de disposición de un ente con una orden Judicial bajo una búsquedaselectiva.

5. Principio de Integridad de datos: Garantizar la exactitud y la veracidad de los datos, protegiendo los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señalar o informar estas acciones no autorizadas (Recomendaciones X.805 y X.815).

La red de INGEMTEL SAS cuenta con mecanismos de cifrado (encriptación) en los dispositivos detransporte, que garantiza y reducen la posibilidad de que la información de usuario de extremo Transportada, procesada o almacenada por una aplicación de red, sufra la modificación, la supresión, la creación y la reactuación sin autorización. Además cuenta con una red completamente segmentada, que no permite que el tráfico sea interceptado por otro dispositivo de la red sin autorización, garantizando aún más la integridad de la información que viaja por esta.

6. Principio de Disponibilidad: Garantizar que las circunstancias de la red no impidan el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones (Recomendación X.805).

INGEMTEL SAS cuenta con un esquema de operación redundante en puntos críticos de la red principalmente en la red CORE, contando con al menos dos proveedores de capacidad en salida hacia Internet, equipos de red de contingencia y archivos de configuración y de información guardados en copias de seguridad, listos para ser restablecidos en el menor tiempo posible en caso de falla de alguno de los elementos que componen la red de transporte de datos.

7. Phishing: El "phishing" es una modalidad de estafa diseñada con la finalidad de robarle al usuario su identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

Como funciona:

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como un banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales. Para que estos mensajes parezcan aún más reales, el estafador suele incluir un vínculo (link) falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Como Protegerse:

Este tipo de fraude debe contenerse a través del ISP y vía usuario.

El usuario debe seguir estas recomendaciones para evitar que sea víctima de robo de su identidad:

Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje. Tener especial cuidado en correos que supuestamente han sido enviados por entidades financieras y compras por Internet, como eBay, PayPal, bancos, etc. Solicitando actualizar datos de cuentas y/o accesos, ya que ninguna de estas entidades solicitan este tipo de información por este medio.

Asegúrese que su PC cuente con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes (Microsoft, Mac, etc.....)

Para visitar sitios Web, introduzca directamente la dirección URL en la barra dedirecciones.

Asegúrese de que el sitio Web utiliza cifrado.

Si tiene instalado servidores Web, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes. Muchas veces los phishers buscan en la red servidores Web vulnerables que puedan ser utilizados para montar páginas que intentan suplantar la identidad de una entidad financiera, sin que el usuario se dé cuenta.

Para el cliente, esto tiene como repercusión la afectación directa en su servicio de Internet, ya que la IP donde se encuentra alojada la página fraude es reportada por entidades internacionales pidiendo al ISP (INGEMTEL SAS) el bloqueo de la misma. Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

A nivel del ISP, actualmente INGEMTEL SAS implementa filtros anti-spam que ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el phishing recibidos por el usuario.

8. Spam: Se llama spam, correo basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera a los usuarios que reciben este correo. Aunque su difusión se puede hacerse por distintas vías, lo más común es hacerlo vía correo electrónico. Actualmente INGEMTEL SAS cuenta con una plataforma que protege a los usuarios de este tipo de correos

Normas básicas para evitar y reducir al mínimo el spam

El spam es un problema que debe ser controlado desde diferentes frentes, tanto a nivel de usuarioscomo a nivel de los proveedores de Internet.

A nivel de usuario, se pueden seguir estas recomendaciones para evitar ser inundadopor correo spam:

Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si ustedtiene un software bloqueador de spam y/o filtro de aplicación ejecutándose en su PC. Los archivos adjuntos a menudo incluyen software o aplicaciones malintencionadas que pueden tener efectos muy negativos sobre su PC, desde borrar su información más valiosa hasta capturar contraseñas, números detarjetas de crédito, etc sin que el usuario ni siquiera se entere. Estas aplicaciones no se pueden incluir en un mensaje de correo electrónico en texto plano, la cual es la razón por la que se empaquetan en losarchivos adjuntos.

Si recibe un correo spam, nunca haga clic en el vínculo “Quitar spam”, ya que lo que buscan los spammers es que el cliente verifique que esta dirección de correo está activa, añadiendo posiblemente su cuenta de correo a más y más listas de spam, lo cual ocasionará que usted reciba mayor cantidad decorreo no deseado.

Algunos programas que utilizan los spammers tratan de adivinar las cuentas de correo a las cuales enviar correo no deseado, por lo cual es recomendable utilizar cuentas que contengas números y letras para que no sean fácilmente ubicadas.

Nunca dar click sobre enlaces (links) que se encuentren dentro de un mensaje de correo electrónico de un remitente desconocido. Probablemente pueda ser un caso de phishing para tratar de robar la identidad del usuario o puede activar un programa que silenciosamente descargue aplicaciones en su PC.

En caso de que usted conozca al remitente, igual la recomendación es no dar click sobre enlaces (links)que se encuentren dentro del mensaje. Uno nunca puede estar seguro de que quien envía el mensaje es realmente quien dice ser, ya que los spammers pueden cambiar la cuenta remitente, suplantando la identidad de otra persona.
Para acceder a un enlace (link) dentro del mensaje, se recomienda cerrar el mensaje, y visitar el sitio encuestión, introduciendo manualmente la URL (por ejemplo, www.google.com) en su navegador de Internet. Es la única manera de estar seguro que la página a la cual se está accediendo es la real.

Para tratar de evitar que su cuenta sea ingresada en listas de correo utilizadas por los spammers, se recomienda que el usuario preste cuidado a los sitios donde ingresa y que le solicita registrarse (mediante una cuenta de correo), ya que existen muchos sitios Web inescrupulosos que venden estas cuentas registradas a redes de spammers.

Si tiene instalado servidores de correo, asegúrese que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes.En muchos casos, los servidores de correo, debido a configuraciones deficientes, permiten que cualquier persona, desde Internet, utilice estos servidores para enviar correos (conocido como Open Relay), afectando el servicio de correo del cliente y muy posiblemente será bloqueado en listas negras de Spam mantenidas a nivel mundial.

En caso que usted como cliente tenga problemas en el envío de correos, para verificar que su IP no seencuentra reportada en listas negras de spam, puede revisar los siguientes enlaces para realizar la consulta:

http://www.dnsstuff.com/

Para que pueda ser efectivo este desbloqueo, el cliente deberá tomar las medidas correspondientes para evitar que se continúe enviando correo spam.

Hay que tener en cuenta que el tiempo de desbloqueo depende del sitio en el cual ha sido reportada una IP.

Entre los sitios más frecuentes, están:

- www.aol.com: Tiempo de desbloqueo aprox. 48horas
- www.lashback.com: Tiempo de desbloqueo aprox. 1hora
- www.uceprotect.net: Tiempo de desbloqueo aprox. 7días
- www.spamcop.net: Tiempo de desbloqueo aprox. 24horas
- www.dsbl.org: Tiempo de desbloqueo aprox. 7dias
- www.wpbl.info: Tiempo de desbloqueo aprox. 1hora
- www.moensted.dk: Tiempo de desbloqueo aprox. 1hora
- www.comcast.com: Tiempo de desbloqueo aprox. 48horas
- www.abuso.cantv.net: Tiempo de desbloqueo aprox.48 horas
- www.spamhaus.org: Tiempo de desbloqueo aprox. 24 horas

A nivel del ISP, actualmente INGEMTEL SAS implementa filtros anti-spam que ayudan a proteger a losusuarios y bloquean las direcciones IP que están enviando correos sospechosamente masivos por un periodo de tiempo.

9.Virus Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del PC, sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos almacenados en un PC aunque también existen otrosmás "benignos", que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráficoinútil.

Como Protegerse:

Similar al spam, los virus son un problema que debe ser controlado desde diferentes frentes, tanto a nivel de usuarios como a nivel de los proveedores de Internet. A nivel de usuario, se pueden seguir estas recomendaciones para evitar ser víctima de los efectos de un virus informático:

Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si usted tiene un software antivirus y/o filtro de aplicación ejecutándose en su PC. Los archivos adjuntos a menudo incluyen software o aplicaciones malintencionadas que pueden tener efectos muy negativos sobre su PC.

Evite caer en técnicas conocidas como de Ingeniería social en la cual llega un correo electrónico con un mensaje del estilo “ejecute este programa y gane un premio”.

Evitar la instalación de software pirata o de baja calidad, mediante la utilización de redes P2P, ya que muchas veces, existen ciertos sitios que “prometen” la descarga de un aplicativo en particular pero en realidad lo que el usuario descarga es un virus.

Asegurarse que su equipo PC cuente con las últimas actualizaciones a nivel de seguridad tanto a nivelde sistema operativo como de los aplicativos instalados, dadas por el fabricante. Existen algunos tipos de virus que se propagan sin la intervención de los clientes y que aprovechan debilidades de seguridadde los diferentes sistemas y aplicaciones, como por ejemplo los virus Blaster y Sasser.

Instalar software antivirus en el PC, el cual esté actualizado con las últimas firmas dadas por el fabricante respectivo.

A nivel de ISP, INGEMTEL SAS cuenta con un Firewall de borde especializado en detectar los virus máscomunes identificándolos por las direcciones IP y puertos específicos de red que utilizan la mayoría de estos, bloqueando así el acceso o salida por un periodo de tiempo.