SEGURIDAD EN LA RED

La empresa **NICE COMUNICACIONES SAS** como proveedor de servicios de telecomunicaciones está convencido que para mantener una relación sana y asertiva con sus clientes la mejor manera es manteniendo una comunicación clara de los servicios que ofrece y brindando información clara de las formas de seguridad que aplica la empresa en la red y además explicando al cliente la forma en que este nos puede ayudar a fortalecer la seguridad de la red.

Por tal motivo a continuación brindamos información de seguridad en la red.

Lo Importante es proteger la información. Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información.

Confidencialidad La confidencialidad o privacidad es el más obvio del aspecto y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas" la intercepción o recepcion electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

Integridad La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre

Disponibilidad La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

PROBLEMÁTICA

La red Mundial de Internet cada día se vuelve más insegura debido a que Miles de computadoras conectadas a Internet, en promedio varias horas por día, con velocidades importantes y con capacidades de procesamiento apreciables son tentadoras para los atacantes La seguridad de las computadoras hogareñas no es una prioridad de la mayoría de la población

•En general, en seguridad, se es “reactivo”.

Los sistemas operativos no son seguros.

•Las aplicaciones no son seguras.

•Desde que se conoce una vulnerabilidad hasta que se desarrolla el parche que la corrige puede pasar un tiempo apreciable (días, meses,...) y hasta que se aplica más aún (¿años?)

•Estamos rodeados de–Intentosde robode identidad

•Phishing

•Pharming–Virus, spyware

y otros malwares BotNets–Intentosde denegaciónde servicio

MECANISMOS DE SEGURIDAD

NICE COMUNICACIONES SAS cuenta con sistema de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que controles de autenticación para los usuarios (equipos terminales de acceso del cliente).

NICE COMUNICACIONES SAS cuenta con diferentes protecciones para controlar el acceso a los servicios de Internet tales como los mecanismos de identificación y autorización respecto a los servicios. Para proteger las plataformas de los servicios de Internet, NICE COMUNICACIONES SAS ha implementado configuraciones de seguridad base en los

diferentes equipos de red, lo que comúnmente se llama líneas base de seguridad, además del establecimiento de medidas de seguridad a través de elementos de control y protección como:

Firewall: A través de éste elemento de red se hace la primer protección perimetral en las redes de NICE

COMUNICACIONES SAS y sus clientes, 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 en NICE COMUNICACIONES SAS son protegidos mediante sistemas anti códigos maliciosos.

Antiespam: Todos los servidores de correo poseen antiespam que reduce el nive de correo basura o no solicitado hacia los clientes, descngestionando los buzones y el tráfico en la red.

Filtrado de URLs: Se realiza filtrado de URLs a los clientes que asi lo soliciten por medio de su equipo final, además NICE COMUNIACIONES SAS cuenta con varios mecanismos capaces de realizar el bloqueo de URLs, entre ellos se encuentran los los sistemas DNS y una herramienta para todo el trafico hacia internet. Además se tiene como objetivo principal el bloqueo de paginas que contengan o promuevan la pornografía infantil en internet a través de imágenes, textos, documentos, textos, y/o archivos audiovisuales.

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 eso se permite hace una conexiona internet mas segura.

AMENAZAS TECNICAS DE SEGURIDAD

- **Malware.** Es el acrónimo, en inglés, de las palabras 'malicious' y 'software', por lo que se conoce como software malicioso. En este grupo se encuentran los virus clásicos (aquellas formas de infección que existen desde hace años) y otras nuevas amenazas que han surgido con el tiempo. S**e puede considerar como malware todo programa con algún fin dañino** (hay algunos que incluso combinan diferentes características de cada amenaza).

- **Spam.** Es el correo electrónico no deseado o correo basura, que se envía sin ser solicitado, de manera masiva, por parte de un tercero. Aunque en un principio se utilizaba para envío de publicidad, se ha visto un creciente uso con el fin de propagar códigos maliciosos. Según estudios, **entre el 80 y el 85% del correo electrónico que se le envía a una persona es correo basura.** El spam llegaba a la bandeja de entrada inicialmente en mensajes en formato de texto. Sin embarg , con la creación de filtros anti-spam, el spam evolucionó a correos con imágenes o contenido Html para evadir la protección.

- **Virus.** Es un programa informático creado para producir algún daño en el computador. **Posee dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo**, acciones que pueden compararse con los virus biológicos que producen enfermedades (y un daño) en las personas, actúan por sí solos y se reproducen (contagian).

  Los virus pueden infectar de dos maneras diferentes. La tradicional consiste en 'inyectar' una porción de código malicioso en un archivo normal. Es decir, el virus reside dentro del archivo ya existente. De esta forma, cuando el usuario ejecute el archivo, además de las acciones normales del archivo en cuestión, se ejecutan las instrucciones del virus. La segunda forma de infectar consiste en "ocupar el lugar" del archivo original y renombrar este por un nombre conocido solo por el virus. En este caso, al ejecutar el archivo primero se ejecuta el malicioso y, al finalizar las instrucciones, este llama al archivo original, ahora renombrado.

- **Spyware.** Los programas espía **son aplicaciones que recopilan información del usuario sin su consentimiento.** Su objetivo más común es obtener datos sobre los hábitos de navegación o comportamiento en la web del usuario atacado y enviarlos a entes externos. Entre la información recabada se puede encontrar qué sitios web visita, cada cuánto lo hace, cuánto tiempo permanece el usuario en el sitio, qué aplicaciones se ejecutan, qué compras se realizan o qué archivos se descargan.

  No es una amenaza que dañe al ordenador, sino que afecta el rendimiento de este y, en este caso, atenta contra la privacidad de los usuarios. Sin embargo, en algunos casos se producen pequeñas alteraciones en la

  configuración del sistema, especialmente en las configuraciones de Internet o en la página de inicio.

- **Phishing.** Consiste en el robo de información personal y financiera del usuario, a través de la falsificación de un ente de confianza. **El usuario recibe un correo electrónico simulando la identidad de una organización de confianza, por lo que este, al confiar en el remitente, envía sus datos directamente al atacante.** Su

  identificación es compleja pues prácticamente todos los componentes del mensaje enviado al usuario son idénticos a un mensaje legítimo del mismo tipo.

- **Ingeniería social.** Es una acción o conducta social destinada a c**onseguir información de las personas cercanas a un sistema por medio de habilidades sociales.** Con esto se busca que el usuario comprometa al sistema y revele información valiosa por medio de variados tipos de engaños, tretas y artimañas.

  Por ejemplo, el usuario es tentado a realizar una acción necesaria para vulnerar o dañar un sistema, cuando recibe un mensaje que lo lleva a abrir un archivo adjunto. O puede suceder que el usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos, en el caso del scam y el phishing.

- **Adware.** Su nombre se deriva de la combinación de las palabras ADvertisement (anuncio) y softWARE). Se trata de un **programa malicioso que se instala en el computador sin que el usuario lo note, y cuya función es descargar y mostrar anuncios publicitarios en la pantalla de la víctima** (se ven como ventanas emergentes del navegador o pueden aparecer incluso si el usuario no está navegando por Internet).

  El adware no produce una modificación explícita que dañe el sistema operativo, pero sí disminuye el rendimiento del equipo y de la navegación por la Red ya que utiliza recursos del procesador, la memoria y el ancho de banda. Por lo general, el adware utiliza información recopilada por algún spyware para decidir qué publicidad mostrar.

  - **Botnets.** Es una red de equipos infectados (robot o zombi) por códigos maliciosos, los cuales son controlados por un delicuente informático el cual, de manera remota, envía órdenes a los equipos zombis haciendo uso de sus recursos. **Las acciones de un equipo zombi son realizadas en su totalidad de forma transparente al usuario.** Por este motivo, uno de los síntomas más importantes de un sistema infectado por un malware de este tipo es el consumo excesivo de recursos, el cual hace lento el funcionamiento del sistema y de las conexiones, e incluso puede llegar a impedir su utilización.

    Los dueños de redes botnets las utilizan para acciones como envío de spam, ataques a sitios web, alojamiento de archivos para sitios web (material pornográfico, cracks, sitios de phishing, etc.), distribución e instalación de nuevo malware y abuso de publicidad en línea.

  - **Gusanos.** Son un sub-conjunto de malware. **Su principal diferencia con los virus tradicionales es que no necesitan de un archivo anfitrión para seguir vivos**, por lo que se reproducen utilizando diferentes medios como las redes locales o el correo electrónico. El archivo malicioso puede copiarse de una carpeta a otra o enviarse a toda la lista de contactos del correo electrónico, citando solo algunos ejemplos.

    La segunda diferencia es que su objetivo no es necesariamente provocar un daño al sistema, sino copiarse a la mayor cantidad de equipos como sea posible. En algunos casos, los gusanos transportan otros tipos de malware, como troyanos o rootkits; en otros, simplemente intentan agotar los recursos del sistema como memoria o ancho de banda mientras intenta distribuirse e infectar más ordenadores.

  - **Troyanos.** Su nombre proviene de la leyenda del caballo de Troya, pues **se disfraza para engañar al usuario: Los archivos que simulan ser normales e indefensos,** como pueden ser juegos o programas, provocan al usuario para ue los ejecute y así logran instalarse en los sistemas. Una vez ejecutados, parecen realizar tareas

inofensivas pero paralelamente realizan otras tareas ocultas en el ordenador.

Al igual que los gusanos, no siempre son malignos o dañinos. Sin embargo, **a diferencia de los gusanos y los virus, estos no pueden replicarse por sí mismos**. A través de un troyano un atacante pueda conectarse

remotamente al equipo infectado, registrar el tipeo y robar contraseñas, y hasta robar información del sistema. Entre los disfraces más comunes que utilizan los troyanos se encuentran archivos por correo electrónico que simulan ser una imagen, un archivo de música o algún archivo similar, legitimo e inofensivo.

- **Scam.** Es el nombre utilizado para las **estafas a través de medios tecnológicos**. Los medios utilizados por el scam son similares a los que utiliza el phishing, si bien su objetivo no es obtener datos sino lucrar de forma directa a través del engaño. Las técnicas más comunes son el anuncio de una ganancia extraordinaria o las peticiones de ayuda caritativa.

- **Rootkit.** Son herramientas como programas, archivos, procesos, puertos o cualquier componente lógico diseñadas para **mantener en forma encubierta el control de un computador.** No es un software maligno en sí mismo, sino que permite ocultar las acciones malignas que se desarrollan en un equipo. Otras amenazas se incorporan y fusionan con técnicas de rootkit para disminuir su probabilidad de ser detectadas.

ENFOQUE EN PHISHING, SPAM, VIRUS.

PHISHING:

Definición: 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 el 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 de direcciones.

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 e 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 de 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 (Telmex Hogar) el bloqueo de la misma.

Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

A nivel del ISP, actualmente NICE COMUNICACIONES 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.

SPAM

Definición:

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 ví s, lo mas común es hacerlo vía correo electrónico.

Actualmente NICE COMUNICACIONES 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 usuarios como a nivel de los proveedores de Internet.

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

Si no se reconoce un remitente de un correo, no abrir los archivos adjuntos del mensaje, incluso si usted tiene 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 mas valiosa hasta capturar contraseñas, números de tarjetas 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 los archivos 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 de correo 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 en cuestión, 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 ud como cliente tenga problemas en el envío de correos, para verificar que su IP no se encuentra reportada en listas negras de spam, puede revisar los siguientes enlaces para realizar la consulta:

https://mxtoolbox.com/blacklists.aspx

En caso que su IP se encuentre reportada acceder al siguiente enlace para tramitar el desbloqueo:

https://check.spamhaus.org/

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 reportado una IP. Entre los sitios más frecuentes, están:

www.aol.com: Tiempo de desbloqueo aprox. 48 horas

www.lashback.com: Tiempo de desbloqueo aprox. 1 hora

www.uceprotect.net: Tiempo de desbloqueo aprox. 7 días

www.spamcop.net: Tiempo de desbloqueo aprox. 24 horas

www.dsbl.org: Tiempo de desbloqueo aprox. 7 días

WWW.WPBL.INFO: Tiempo de desbloqueo aprox. 1 hora

WWW.MOENSTED.DK: Tiempo de desbloqueo aprox. 1 hora

www.comcast.com: Tiempo de desbloqueo aprox. 48 horas

www.abuso.cantv.net: Tiempo de desbloqueo aprox.48 horas

www.spamhaus.org: Tiempo de desbloqueo aprox. 24 horas

VIRUS

Definición: 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 otros más "benignos", que solo se caracterizan por ser molestos.

Los virus informáticos t enen, 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 tráfico inútil.

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 nivel de 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 seguridad de 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, NICE COMUNICACIONES SAS cuenta actualmente con equipos especializados en la detección y filtrado de correos con virus, mediante filtros de tipo heurístico, firmas de virus reconocidos y adicional cuenta con filtros de tipo preventivo, que aunque a nivel público no se halla liberado una firma para contener una nueva amenaza, el sistema coloca en cuarentena este tipo de tráfico, hasta determinar si el tráfico es legal o hasta que se tenga la firma correspondiente a la propagación del nuevo virus o gusano. Todos los correos que los usuarios reciben y envían son filtrados por esta herramienta.

Fuentes.

Conceptos Básicos de Seguridad Informática. http://www.bradanovic.cl/pcasual/ayuda3.html

Amenazas Técnicas Informáticas. http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/

Phishing, Spam, Virus. http://www.claro.com.co/wps/wcm/connect/co/claro2013.colombia/pc/personas/legal-y-regulatorio/lightbox-fijo/phishing

Seguridad en la Web. http://www.mediacommerce.net.co/seguridad-en-la-web/