«Todo lo que necesita saber para evitar amenazas en la red, y llevar a cabo una navegación segura«

Tipos de amenazas en la red

Para L3 ACCESS S.A.S su seguridad en la red es muy importante, por tal razón en este documento encontrará información de su interés para una navegación segura:

Malware

Es un término general que se utiliza para referirse a distintas formas de software hostil, intrusivo o molesto.

El software malintencionado o malware es un software creado por hackers para perturbar las operaciones de una computadora, obtener información confidencial o acceder a sistemas informáticos privados.

El malware incluye virus informáticos, gusanos, troyanos, spyware, adware, la mayoría de rootkits y otros programas malintencionados.

Las siguientes son algunas formas de software malintencionado:

Spyware

es un tipo de malware (software malintencionado) que se instala en las computadoras para obtener información sobre los usuarios sin que éstos lo sepan. El spyware suele estar oculto al usuario y puede ser difícil de detectar. Algunos spywares, como los keyloggers —registradores de teclas—, pueden ser instalados de forma intencionada por el propietario de una computadora de uso común, corporativo o público para controlar a los usuarios.

Aunque el término “spyware” sugiere un software que espía las actividades de un usuario en una computadora, las funciones del spyware pueden ir mucho más allá y llegar hasta la obtención de casi cualquier tipo de datos, incluida información personal como hábitos de navegación en Internet, accesos de usuarios o datos de crédito y cuentas bancarias. El spyware también puede interferir con el control de una computadora por parte del usuario, instalando nuevo software o redirigiendo a los navegadores web. Algunos spywares tienen capacidad para modificar la configuración de una computadora, lo que puede tener como consecuencia una menor velocidad de conexión a Internet y cambios no autorizados en la configuración de navegadores u otro software.

Spam

consiste en el uso de sistemas de mensajes electrónicos para enviar de forma indiscriminada un gran número de mensajes no solicitados. Aunque la forma más conocida de spam es el de correo electrónico, el término se aplica también a abusos similares en otros medios: spam de mensajes instantáneos, spam de grupos de noticias de Usenet, spam de motores de búsqueda en la web, spam en blogs, spam en wikis, spam en anuncios clasificados de Internet, spam de mensajes de teléfonos móviles, spam en foros de Internet, transmisiones fraudulentas por fax, spam en redes sociales, publicidad en televisión y spam en redes de uso compartido de archivos.

Phishing

consiste en el intento de adquirir información (y, en ocasiones, también de dinero, aunque sea de forma indirecta), como nombres de usuarios, contraseñas y datos de tarjetas de crédito haciéndose pasar por una entidad de confianza en una comunicación electrónica. Los correos electrónicos de phishing pueden contener enlaces a páginas web infectadas con malware. La forma más habitual de phishing utiliza mensajes instantáneos o correos electrónicos fraudulentos en los que se pide a los usuarios que introduzcan sus datos en una página web falsa que es casi idéntica a la página auténtica. El phishing es un ejemplo de las técnicas de ingeniería social empleadas para engañar a los usuarios, el cual aprovecha las limitaciones de uso de las actuales tecnologías de seguridad en la web. Entre los intentos de lucha contra el creciente número de incidentes de phishing figuran medidas legislativas, de formación de usuarios, de divulgación y de seguridad técnica.

Pharming

es una forma de ataque cuyo objetivo es redireccionar el tráfico de un sitio web hacia una página fraudulenta. El término “pharming” es un neologismo formado por la unión de las palabras inglesas “phishing” y “farming”. El phishing es una técnica de ingeniería social que pretende obtener datos de acceso, como nombres de usuarios y contraseñas. Tanto el pharming como el phishing se han utilizado en los últimos años con el fin de adquirir información que permita el robo de identidades online. El pharming es ya un problema grave para las empresas de comercio electrónico y banca electrónica.

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.

Mecanismos de Seguridad

L3 ACCESS S.A.S. cuenta con sistemas 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).

L3 ACCESS S.A.S. 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, L3 ACCESS S.A.S 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 primera protección perimetral en las redes de L3 ACCESS S.A.S. 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 L3 ACCESS S.A.S. están protegidos a través de sistemas anti códigos maliciosos.

Antispam:

Todos los 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:

L3 ACCESS S.A.S para el bloqueo de sitios con contenido de pornografía infantil, utiliza Servidores para realizar el filtrado de estos sitios. 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.

Garantía de Seguridad de la Red e Integridad del Servicio

L3 ACCESS S.A.S. mantiene monitoreo constantes en cada uno de los elementos que forman parte técnica de la prestación de los servicios, permitiendo la identificación oportuna de cualquier evento o anomalía en la red. Para ello, utiliza equipos estratégicamente ubicados que monitorean aspectos como:

- Estado de los equipos de red
- Logs de actividades en los equipos
- Comportamiento del tráfico en distintos sectores de la red (puntos de interconexión, peering y nodos)
- Informes de control de Firewall, detallando tráfico en puntos críticos, firmas de ataques, y análisis de vulnerabilidades
- Backups de dispositivos de red, protegidos bajo estructuras de mínima exposición pública

Modelos de Seguridad Adaptados a la Red

L3 ACCESS S.A.S. , cumpliendo con las normativas de vigilancia y control, ha implementado modelos de seguridad específicos para la protección de redes y usuarios, conforme a los estándares UIT:

1. **Autenticación:**
    - Basada en las normas UIT X.805 y X.811, la autenticación verifica la identidad de entidades (personas, servicios, aplicaciones). Los servicios de autenticación de L3 ACCESS S.A.S. utiliza un modelo descentralizado que permite garantizar el acceso individual a equipos específicos con privilegios definidos y evitar riesgos de seguridad masivos que pongan en peligro la integridad completa de la plataforma tecnológica que presta los servicios a nuestros usuarios.
2. **Control de Acceso:**
    - Este control asegura que solo personas y dispositivos autorizados accedan a la red y sus recursos, basándose en las recomendaciones UIT X.810 y X.812. L3 ACCESS S.A.S. aplica medidas de seguridad física y lógica:
3. **Registros de Auditoría**
    - L3 ACCESS S.A.S. mantiene registros de acceso y actividades en la infraestructura de CORE y ACCESO, con periodos de retención definidos en cada equipo
4. **Confidencialidad de Datos**
    - Asegura la privacidad y protección contra accesos no autorizados, usando cifrado y controles de acceso
5. **Privacidad**
    - Las políticas de L3 ACCESS S.A.S. garantizan que la información de usuarios no se divulga sin autorización
6. **Integridad de Datos**
    - Protege contra modificaciones no autorizadas, aplicando actualizaciones de software que mitiguen vulnerabilidades en la infraestructura de red

Medidas de Seguridad para Garantizar Confidencialidad, Integridad y Disponibilidad

Las actividades y métodos descritos garantizan la autenticación, protección y cifrado, así como el monitoreo continuo para identificar amenazas y problemas en la red.

- Medidas contra Interceptación y Violación de Comunicaciones L3 ACCESS S.A.S. implementa controles de acceso y sistemas de detección para monitorear eventos en la red, asegurando acciones ejecutadas y denegadas a usuarios y terceros
- Tratamiento de Incidentes de Seguridad L3 ACCESS S.A.S. realiza análisis forense en situaciones de desastre, con equipos capaces de recuperar información y rastrear eventos. Utiliza sensores y mecanismos de observación en puntos críticos de la red
- Mecanismos para Garantizar Confidencialidad, Integridad y Disponibilidad L3 ACCESS S.A.S. cumple con regulaciones gubernamentales para el manejo de información de usuarios, garantizando la confidencialidad y prevención de fraudes en telecomunicaciones