Empresa de Gases Industriales
Dirección de Informática y Comunicaciones
Avenida Finlay Km 2 ½. Reparto: Puerto Príncipe, Camagüey, Cuba
Teléfonos: 032 264344 y 032 264346
E-mail: ernesto.santana@gases.co.cu

ORDINARIO

Habana, 01 de agosto de 2020
"Año 62 de la Revolución"

A: Todas las entidades de la Empresa de Gases Industriales.

Asunto: Indicación de obligatorio cumplimiento para el correcto uso y configuración del Firewall (Cortafuegos) en la Red de Gases Industriales, como medida de la seguridad para evitar accesos no autorizados y minimizar vulnerabilidades críticas que estos representan.

La Dirección de Informática y Comunicaciones de la Empresa de Gases Industriales de Cuba, teniendo en cuenta que:

- Existen nuevas regulaciones de seguridad informática y se desarrollan inspecciones de entidades externas a nuestras unidades de base, para hacer cumplir estas regulaciones. Ver a continuación algunas regulaciones relacionadas con las inspecciones de externos y las configuraciones tratadas en manual adjunto a la presente indicación, situado en el SVN Configuración del Kerio; pertenecientes a Resolución 128/2019, Decreto Ley 360, Guía de inspección del Minint y Acuerdo No. 33 CIC. La base legal se podrá adquirir en la dirección, SVN Base Legal.
    1. Deficiente segmentación de la red al no establecer VLAN para la separación de los grupos de trabajo en la Organización. **Artículo 54, Decreto 360/19; Medida 3 acápite 3, Acuerdo No. 33 CIC**.
    2. No se aplican en toda su dimensión las medidas de seguridad para restringir el acceso de los usuarios, a los recursos de la red interna desde dispositivos móviles conectados por WiFi. **Resolución 360/19**.
    3. No se tienen implementado sistemas para la detección de ataques contra su infraestructura (interna/externa). **Medida 14, Acuerdo No. 33**.
    4. No se implementan medidas de seguridad para limitar el tráfico de las estaciones de trabajo a los Servidores. **Artículo 44, 45 y 54 Decreto 360/19; Medida 3 acápite 1 y 3, Acuerdo No. 33 CIC**.
    5. Direccionamiento dinámico por el DHCP sin control de la dirección IP, ni la MAC de las PC. **Medida 3 acápite 4, Acuerdo No. 33 CIC**.
    6. No se implementan medidas para el control de las estaciones de trabajo que se conectan a la aplicación. (anclaje por direcciones MAC, IP, correspondencia entre el usuario SSH y la autenticación en la aplicación, configuración de VLAN). **Medida 2, acápite 1, 2, y 4, Medida 3, acápite 3 y 4, Acuerdo No. 33 CIC**.
    7. No se establece una política de filtrado que permita controlar el acceso al dominio mediante el anclaje del usuario o Grupos con la dirección IP y la MAC. **Medida 3, acápite 2 y 4, Acuerdo No. 33 CIC**.
    8. No se tienen implementada una DMZ[1] entre la sub-red de usuarios y los servicios que se consumen. **Artículo 39, resolución 128/19. Zona desmilitarizada**.
    9. Se encuentran habilitados varios enlaces inalámbricos con acceso a la red de la entidad. **Medida 5, Acuerdo No. 33**.

10. Presencia de puntos de acceso inalámbricos conectados al segmento de red corporativo sin el debido control y seguridad. **Medidas 3 y 5, Acuerdo No. 33**
11. Incorrecta implementación en el equipamiento que garantiza la seguridad en el perímetro de red. **Reglamentos 128 y 129/19, Decreto 360/19 del MINCOM, Acuerdo 33 CIC**.
12. Se determinó la presencia de tecnología obsoleta para el control del perímetro de la red. **Decreto 360/19 del MINCOM, Acuerdo 33 CIC**.
13. No se realizan acciones de control al tráfico que se genera hacia el sistema de contabilidad. **Artículos 42 y 54 del Decreto 360/19 del Mincom; Medida 2, acápite 4 del Acuerdo No. 33 CIC**.
14. **Resolución 126/2019 Resuelvo QUINTO:** Las herramientas de seguridad, de las cuales se brinda información sobre sus funciones en el anexo que es parte integrante de la presente Resolución, cumplen los objetivos siguientes:
    a) Mostrar el estado actualizado de los servicios implementados en cada servidor;
    b) supervisar la carga y disponibilidad de los servidores;
    c) establecer un Sistema de Detección y Prevención de Intrusos, por sus siglas en inglés IDS/IPS;
    d) monitorear el comportamiento del tráfico de la red, análisis de protocolos y detección de anomalías;
    e) dar seguimiento a las trazas;
    f) detectar posibles vulnerabilidades en la red;
    g) controlar centralizadamente el estado físico del hardware y del software;
    h) gestionar las actualizaciones de seguridad;
    i) establecer un sistema de correlación de eventos;
    j) realizar el aviso oportuno ante la detección de anomalías o eventos de ciberseguridad.
15. **Resolución 128/2019 Artículo 36.** El administrador de una red informática tiene, en relación con la seguridad de las TIC, los deberes siguientes:
    a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red;
    b) realizar el análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red;
    c) garantizar que los servicios implementados sean utilizados para los fines que fueron creados;
    d) comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes;
    e) activar los mecanismos técnicos y organizativos de respuesta ante distintos tipos de incidentes y acciones nocivas que se identifiquen, y preservar toda la información requerida para su esclarecimiento;
    f) participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas;
    g) informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento;

h) garantizar que en el registro de trazas se incluya las relacionadas con la navegación a Internet, que permitan correlacionar la dirección IP real de salida al proveedor de servicios de Internet, con las IP privadas empleadas en las redes internas de la entidad;
i) participar en la confección y actualización del Plan de Seguridad de las TIC;
j) implementar y operar los controles que se establezcan para gestionar los riesgos de seguridad.

- Es una necesidad para la red de Gases Industriales estandarizar la Aplicación Firewall, así como las versiones de esta utilizada en las UEBs; con el objetivo de dar soporte a este servicio desde el Nodo o cualquier unidad ante fallas y/o la no existencia de un administrador de red y por el chequeo de las auditorías automáticas realizadas a este aspecto.
- Se desconocen: muchos aspectos de los cortafuegos, que configurados incorrectamente pueden afectar las redes; la configuración y salvas de estos y no existe un control exhaustivo de todas las reglas de acceso en las entidades de base.
- Es obligación y responsabilidad de los Especialistas de seguridad informática y Administradores de Red de las unidades la correcta configuración del firewall.

Resuelve:

1. Como parte de la mejora de la arquitectura de red de las UEBs se debe, estandarizar la aplicación Firewall a Kerio Control versión 9.0 o superiores en todas las unidades de gases industriales, así como, la instalación del **Kerio Control en una máquina virtual que separe las funciones de filtrado de los demás servidores de las UEBs**.

2. Estandarizar la configuración de los aspectos más significativos de Kerio Control.

3. Chequear la configuración del Firewall en las unidades de base, detectando por las auditorías automáticas, reinstalaciones y cambios de los aspectos estandarizados que puedan acarrear fallas de seguridad. En los aspectos técnicos de auditorías la configuración del Kerio Control, aparecerá como otra fila en la Tabla Roja-Verde con el título: Kerio, errores de configuración.

4. Migrar el servicio DHCP hacia el Kerio en todas las unidades y eliminar este servicio en los servidores Windows, así como configurar correctamente la salva de los logs para que la rotación semanal no afecte el salvado de estos ni exista pérdida de datos, esto facilita:

    a. Filtrado de MAC en el Kerio Control cuando este presta el servicio DHCP.

    b. Salva de los logs del DHCP al salvar todos los logs del Kerio Control.

5. Solucionar el señalamiento de filtrado de MACs, orientado por entidades externas en inspecciones; para la reserva de IP a todas las estaciones de trabajo en el DHCP. De esta forma todo el personal que se conecte en las unidades y no pertenezca a ella o se encuentre fuera de su puesto contactará a los administradores, para obtener IP y poder alcanzar los servicios de la red. Ver aspectos en punto 1.

Empresa de Gases Industriales
Dirección de Informática y Comunicaciones
Avenida Finlay Km 2 ½. Reparto: Puerto Príncipe, Camagüey, Cuba
Teléfonos: 032 264344 y 032 264346
E-mail: ernesto.santana@gases.co.cu

6. Dar solución al señalamiento de entidades externas en inspecciones por no contar con alertas del IPS.
7. Se deberán configurar las salvas de los logs del Firewall Kerio Control hacia un SYSLOG server en todas las UEBs.
8. Los aspectos a estandarizar se verán descritos en el Manual de Configuración de Kerio Control adjunto a la presente indicación. Cualquier otro aspecto que deba configurarse será añadido al manual y divulgado nuevamente, los nuevos aspectos pueden proceder de inspecciones de entidades externas u orientaciones de base legal.
9. La presente indicación podrá ser accedida en la carpeta del svn, Indicaciones, con el nombre 202007-0002_cortafuegos_config_ueb.
10. **Entrará en vigor a partir del 1 de agosto del 2020.**

Nota: En el caso de las UEBs que no separan la red en VLANs no es posible el cumplimiento de los aspectos expuestos como 1,4,8 y 13 del presente documento que pertenecen a la guía del Minint, aunque se separe la red WiFi como se encuentra en algunas entidades implementado. Para la separación de la red en VLANs es necesario el uso de swicht gestionables.

Aprobado por:

Ernesto Santana Rodríguez
Director de Informática y Comunicaciones
Empresa de Gases Industriales

DIC-0002/20
C.C: Archivo, Emir Sánchez, Lázaro Peña, Adianis Sifontes.