Marzo 2025

NEWSLETTER BeIT

Edición Semanal #24

01 Blog CEO

Field Services 2.0 potencia a las empresas de Facility Management

02 Ciberseguridad en la Nube

Estrategias para proteger entornos híbridos.

03 Eventos

Galería de eventos 2025.

04 Resumen de la siguiente edición semanal

Ciberseguridad en la Nube

La nube es una superficie de ataque en constante desarrollo y evolución. Para defender este entorno de los crecientes ataques, es preciso conocer en profundidad la actividad de los ciberdelincuentes.

Los ciberdelincuentes entienden bien la nube y perfeccionan sus tácticas para abusar de sus servicios y aprovechar sus vulnerabilidades.

Leer ahora

Field Services 2.0 potencia a las empresas de Facility Management

Por: Elías Cedillo , *CEO Grupo BeIT y BuróMC*

La gestión de servicios de campo ha evolucionado significativamente. Field Services 2.0 representa una transformación en la manera en que las empresas de Facility Management operan, ofreciendo mayor eficiencia, flexibilidad y satisfacción del cliente. Esta evolución está impulsando a las empresas a adoptar nuevas tecnologías y estrategias para mantenerse competitivas.

En México, el mercado de Facility Management está en crecimiento, impulsado por la demanda de servicios más eficientes y la adopción de nuevas tecnologías. Según un informe de Mordor Intelligence, se espera que el mercado de Facility Management en México crezca a una tasa compuesta anual del 5.2% entre 2023 y 2028.

McKinsey, en el artículo publicado ¨**Gestión del rendimiento 2.0:** Optimización tecnológica de las fuerzas de campo, 2020. Hace referencia a que las empresas con grandes fuerzas de campo tienen más razones que nunca para aumentar la eficacia y la eficiencia. Las nuevas opciones tecnológicas pueden ayudar a romper las viejas barreras para un mayor rendimiento, brindando beneficios como:

- **Mayor eficiencia operativa**
  - Automatización de procesos.
  - Reducción del tiempo de inactividad.

- **Mejora en la satisfacción del cliente**
  - Resolución rápida y precisa de problemas.
  - Soporte remoto y soluciones móviles.
  - Reducción de tiempos de respuesta.

- **Reducción de costos**
  - Minimización del tiempo de viaje.
  - Mantenimiento predictivo y preventivo.

Las soluciones que ofrece Grupo BeIT y Buró MC, con Field Services 2.0 enfocado a ciberseguridad, subraya la importancia crítica de los servicios de campo dentro de cualquier corporación, incluso en un entorno donde la centralización y la automatización juegan roles dominantes. La eficacia de las soluciones basadas en la nube y la gestión centralizada, el contacto físico con los activos sigue siendo indispensable. Esta necesidad se fundamenta en el papel esencial de los equipos informáticos actualizados y seguros como pilares de la operatividad empresarial.

En **2023 CrowdStrike** en su artículo ¨**Principales técnicas de ataque a la nube y cómo defenderse de ellas¨,** hizo referencia que la identidad, era el nuevo perímetro, y que abría la puerta del reino (información de los usuarios). Los ciberdelincuentes perdieron el interés por desactivar las tecnologías de los antivirus y firewall, y empezaron a centrarse en modificar los procesos de autenticación y atacar las identidades. La adopción continua de aplicaciones y servicios basados en la nube aumenta el número de identidades que un ciberdelincuente puede vulnerar y utilizar en su propio beneficio.

En el **43 % de las intrusiones en la nube**, se utilizaron cuentas de usuarios legítimos para obtener acceso inicia

El **47 % de los errores graves de configuración de la nube** están relacionados con una higiene insuficiente de las identidades y los derechos

CrowdStrike, 'Insiders Guide' (2023)

Ciberseguridad en la Nube

Estrategias para proteger entornos híbridos

NEWSLETTER BeIT
Edición Semanal

La ciberseguridad en la nube es esencial para las empresas que buscan aprovechar las ventajas de la computación en la nube sin comprometer la seguridad de sus datos. Con la creciente adopción de entornos híbridos, que combinan infraestructura local y servicios en la nube, es crucial implementar estrategias robustas para proteger estos entornos.

¿Qué es la Ciberseguridad en la Nube?
La ciberseguridad en la nube se refiere a la protección de sistemas, aplicaciones y datos alojados en la nube mediante tecnologías, protocolos y buenas prácticas que garantizan la integridad y privacidad de la información.

Desafíos de la ciberseguridad en entornos híbridos
Los entornos híbridos presentan desafíos únicos debido a la dispersión de datos y servicios en múltiples plataformas. La seguridad debe ser gestionada de manera integral para evitar vulnerabilidades que puedan ser explotadas por cibercriminales.

Estrategias para proteger entornos híbridos

1. Estrategia de seguridad integrada y visibilidad centralizada
Huawei recomienda establecer una estrategia de seguridad integrada que permita una gestión centralizada de la visibilidad, políticas de seguridad y respuesta a incidentes en toda la infraestructura. Utilizar herramientas de gestión de seguridad como SIEM (Security Information and Event Management) puede ayudar a monitorizar eventos y alertas de seguridad en tiempo real.

2. Implementación del modelo Zero Trust
El modelo Zero Trust, promovido por Huawei, asume que todas las conexiones, internas o externas, pueden representar un riesgo. Implementar autenticación multifactor (MFA) y gestión de identidades y accesos (IAM) es crucial para proteger las identidades y asegurar que solo los usuarios autorizados puedan acceder a los recursos de la empresa.

3. Cifrado de Datos y Gestión de Claves
La protección de los datos es crítica en entornos híbridos. Huawei Cloud utiliza cifrado de datos y una gestión adecuada de claves para asegurar que la información esté protegida tanto en tránsito como en reposo.

4. Fortalecimiento de los puntos de acceso
Los dispositivos conectados son la primera línea de defensa contra las amenazas cibernéticas. Mantener sistemas y aplicaciones actualizados, adoptar autenticación robusta y monitorear constantemente el comportamiento de los dispositivos son pasos esenciales para minimizar riesgos.

Situación actual de la Ciberseguridad en México
En México, la ciberseguridad se ha convertido en una prioridad estratégica debido al aumento de los ciberataques. Durante la primera mitad de 2024, México registró aproximadamente 31 mil millones de intentos de delitos cibernéticos, representando el 55% de las amenazas cibernéticas en América Latina.

Los sectores más afectados incluyen manufactura, salud y construcción, con un notable incremento en ataques de ransomware y phishing.

Cómo Huawei Cloud ayuda: Procesamiento, Almacenamiento, Respaldos, Redes y Consumo

- **Procesamiento**

Huawei Cloud ofrece servicios de procesamiento de alto rendimiento a través de su MapReduce Service (MRS), que incluye componentes de big data como Hadoop, Spark y Flink. Estos servicios permiten el análisis de grandes volúmenes de datos con alta disponibilidad y escalabilidad.

- **Almacenamiento**

El Object Storage Service (OBS) de Huawei Cloud proporciona almacenamiento de objetos escalable y seguro con una durabilidad del 99.9999999999%. Esto permite a las empresas almacenar grandes cantidades de datos de manera económica y segura.

- **Respaldos**

Huawei Cloud ofrece soluciones de respaldo y recuperación a través de su servicio Cloud Backup and Recovery (CBR). Este servicio permite crear copias de respaldo automáticas y restaurar datos rápidamente en caso de fallos, eliminaciones accidentales o ataques de ransomware.

- **Redes**

El servicio Cloud Connect de Huawei Cloud facilita la creación de redes globales rápidas, estables y seguras. Permite la conectividad entre diferentes regiones y redes locales, asegurando una baja latencia y alta disponibilidad.

- **Consumo**

Huawei Cloud proporciona una calculadora de precios que permite a las empresas estimar los costos de sus servicios en la nube. Ofrece opciones de pago por uso y suscripción mensual/anual, lo que permite una gestión flexible y eficiente del presupuesto.

Conclusión

La ciberseguridad en la nube y la protección de entornos híbridos requieren un enfoque proactivo y multifacético. Implementar estrategias como la seguridad integrada, el modelo Zero Trust, el cifrado de datos y el fortalecimiento de puntos de acceso puede ayudar a las empresas a mantener sus datos seguros y garantizar la continuidad operativa en la era digital.

Cómo Grupo BeIT puede ayudarte a abordar la ciberseguridad en la nube y la protección de entornos híbridos mediante un enfoque integral y personalizado. Aquí te explicamos:

1. **Seguridad integrada:** Ofrece soluciones que combinan la seguridad de la red y la nube, asegurando una protección completa de tus datos y sistemas en todos los entornos.
2. **Modelo Zero Trust:** Implementando un enfoque de seguridad de confianza cero, que garantiza que solo los usuarios y dispositivos autorizados puedan acceder a los recursos de la red, minimizando el riesgo de brechas de seguridad.
3. **Cifrado de datos:** Utilizando tecnologías avanzadas de cifrado para proteger tus datos tanto en tránsito como en reposo, asegurando que la información sensible esté siempre segura.
4. **Fortalecimiento de puntos de acceso:** Realizamos auditorías de seguridad y pruebas de penetración para identificar y corregir vulnerabilidades en tus sistemas, fortaleciendo los puntos de acceso y mejorando la resiliencia de tu infraestructura.
5. **Continuidad operativa:** Con nuestras soluciones de ciberseguridad, en colaboración con nuestros partners, tu empresa operaría de manera eficiente y segura.

En Grupo BeIT nos dedicamos proporcionar una protección robusta y eficiente, adaptada a las necesidades específicas de las organizaciones de nuestros clientes, asegurando que sus datos y operaciones.

Referencias:

Huawei Cloud

TECNO EDIFICIOS

El pasado 20 de marzo se celebró el evento **FM's Eficiencia:** *"Implementa estrategias de gestión de tiempo automatizando procesos para el FM"*, en el cual nuestro **CEO, Elías Cedillo**, participó como panelista. El evento contó con la presencia de destacados profesionales como Vladimir Martínez Ríos, Víctor Sierra y Raúl Garcés Hernández. Durante su intervención, nuestro **CEO Elías** compartió su experiencia, conocimientos y estrategias claves para mejorar la eficiencia operativa y optimizar la gestión del tiempo en Facility Management y los servicios de Field Services 2.0.

El pasado martes 19 de marzo, nuestros equipos de Comercial, Marketing, Ingeniería y Soporte, tuvieron la oportunidad de participar en el **webinar de Netskope** *"Descubra cómo optimizar y proteger sus sucursales con Netskope SASE Branch"*.

Durante este evento, los ponentes **Samuel Bonete** y **Danilo Rodríguez** compartieron valiosas perspectivas sobre cómo esta solución avanzada integra capacidades de red y seguridad en una arquitectura basada en la nube. La presentación destacó cómo Netskope SASE Branch puede transformar la gestión de sucursales, ofreciendo una conectividad rápida y segura, y optimizando el rendimiento mientras se reducen los costos operativos.

Este webinar fue una excelente oportunidad para nuestros equipos profundizaran en las innovaciones de Netskope y explorar estrategias para mejorar la eficiencia operativa y la seguridad.

Protección de Infraestructuras

Seguridad en sistemas OT

La protección de infraestructuras críticas es esencial para garantizar la estabilidad y seguridad de servicios vitales como la energía, el agua, las telecomunicaciones y el transporte. En la actualidad donde la digitalización se torna imprescindible, estas infraestructuras están cada vez más expuestas a ciberataques que pueden tener consecuencias devastadoras. La implementación de medidas de seguridad robustas y la colaboración entre sectores públicos y privados son fundamentales para mejorar la ciberresiliencia.

Y Schneider Electric juega ese papel crucial en la protección de infraestructuras y la seguridad en sistemas OT. Ofreciendo una gama de soluciones avanzadas que integran seguridad y control remoto en tiempo real, haciéndolo indispensable para monitorear y proteger las operaciones contra amenazas cibernéticas.