Abril 2025

NEWSLETTER BeIT

Edición Semanal #28

Control de Accesos

Ya no es seguro asumir que un dispositivo conectado a la red debe tener acceso ilimitado. El enfoque de confianza cero garantiza una verificación continua de usuarios y dispositivos que acceden a los recursos. Los dispositivos IoT y de punto final son identificados y protegidos, mientras que los equipos de TI obtienen visibilidad y control total sobre todos los elementos conectados a la red.

Gartner define la gestión de acceso (AM) como herramientas que incluyen capacidades de autenticación e inicio de sesión único (SSO), y que establecen, gestionan y aplican controles de acceso en tiempo de ejecución para aplicaciones web y API clásicas y basadas en estándares.

Leer ahora

Field Services 2.0 de Grupo BeIT

Innovación en la Gestión de Servicios en Campo

Por: Elías Cedillo , *CEO GrupoBeIT*

GrupoBeIT desarrolló su modelo innovador para la gestión de servicios en campo, denominado Field Services 2.0. proyectándose más allá de un Field Services tradicional, dejando de lado una acción reactiva y brindar acciones más proactivas. Respaldado en cuatro pilares fundamentales: Personas, Awareness, Tecnología y Zero Trust Network Access; desde una visión del cumplimiento de normativas de ciberseguridad y protección de la información.

Estrategia Integral Field Services 2.0 Grupo BeIT

Dentro de nuestra ruta de Field Services 2.0 empezamos con el primer pilar las **Personas**; enfocándose en el recurso humano (ingenieros) y la clasificación al modelo de soporte técnico. Este proceso incluye la evaluación del tipo de servicio, la tecnología utilizada, la logística involucrada, y los cambios en los servicios. La correcta clasificación y asignación de tareas aseguran que los ingenieros estén preparados para enfrentar cualquier desafío técnico con eficiencia y precisión tanto en sitio y/o vía remota. McKinsey & Company, en su informe sobre la gestión de tiempo, las empresas pierden en promedio 20-30% de su potencial de productividad debido a su mala gestión. Por otro lado, la Universidad de Stanford encontró que el 75% de los empleados experimentan una pérdida de tiempo debido a interrupciones en su flujo de trabajo, lo que afecta directamente a la capacidad de cumplir con los plazos establecidos.

El segundo pilar es **Awareness**, donde se destaca la importancia de las buenas prácticas. Esto incluye políticas claras, cumplimiento de normativas y medidas de seguridad. La concientización y la adherencia a estas prácticas son esenciales para mantener la integridad y la calidad del servicio, así como para proteger tanto a los empleados como a los clientes.

El cumplimiento de normativas, políticas y medidas de seguridad obliga a una revisión integral de la gobernanza de datos y ofrecer una oportunidad para reimaginar el valor que se les puede proporcionar. Una revisión minuciosa de los datos y de cómo se utilizan, permite a las organizaciones definir su riesgo actual y asegurarse proactivamente que cuentan con los procesos y la arquitectura de seguridad adecuada.

Para ilustrar esto, consideremos el siguiente ejemplo: una aseguradora de salud en EE.UU., valorada en 60,000 millones de dólares, sufrió la violación de 2.8 millones de registros de información de salud protegida (PHI) cuando una computadora portátil fue robada de un proveedor. El impacto total del incidente fue de 1,700 millones de dólares, y casi el 75% de esa cantidad se debió a la pérdida de ingresos por contratos y a la pérdida de la información de la empresa y/o clientes. Ahora que tenemos presente lo que puede involucrar nuestro pilar de Awareness ¿Cómo afectaría a tu organización una violación de datos similar, y qué medidas estás tomando para prevenirlo?

Nuestro tercer pilar, **Tecnología**; pone su atención en la gestión de activos. Este pilar incluye la gobernanza, la seguridad, la visibilidad, y el soporte de los activos tecnológicos. La gestión efectiva de estos recursos garantiza que los servicios en campo se realicen de manera segura y eficiente, proporcionando una base sólida para la operación continua y la mejora constante. En 2024, **KPMG** en su investigación ¨Gestión de Activos en Latinoamérica¨ definió a la gestión de activos como la búsqueda de maximizar el valor de los activos a lo largo de su ciclo de vida, alineando las decisiones de inversión, operación y mantenimiento con los objetivos de la organización. Entre sus resultados obtuvieron que el 51% de los encuestados consideraron que la gestión de activos permite reducir costos operaciones.

Finalmente, **Zero Trust Network Access** el cuarto pilar, centrado en la automatización del control de acceso (confianza 0), asegurando que solo las personas autorizadas puedan acceder a los recursos y aplicativos necesarios. La implementación de este modelo de seguridad es crucial para proteger la infraestructura y los datos sensibles de la organización.

Ahora, retomando el ejemplo anterior y generando un escenario ficticio con las siguientes preguntas ¿Qué clase de nivel de acceso tenía el proveedor? ¿Y qué nivel de acceso tenía el usuario de la laptop? o ¿El equipo contaba con la seguridad adecuada a cada recurso?. En este escenario se puede generar la formula perfecta para que cualquier ciberatacante o intruso puedan realizar una violación digital a la organización, grupo y/o empresa. Imagina por unos minutos que eres el directivo de la empresa del ejemplo anterior. Fortinet en unos de sus informes reveló que el 51% de las organizaciones afirmaron que sus altos directivos se han enfrentado multas (34%), penas de cárcel (16%) y pérdida de posición o empleo (33%) tras un ciberataque. Y a esto sumar que el 62% de los líderes esperan que sus empleados sean víctimas de ciberataques este año 2025 debido a la implementación de IA para mejorar sus métodos para vulnerar. En este caso, la pregunta sería ¿crees que un modelo tradicional aún es eficaz?

	Field Services Tadicional	Field Services 2.0
Gestión de activos de TI	✗	✓
Incremento de la productividad	✗	✓
Capacitación continua operativa de TI	✓	✓
Auditorías de cumplimiento normativo	✗	✓
Evaluación técnica a fuerza operativa	✓	✓
Atención de incidencias en sitio	✓	✓
Homologación de políticas de ciberseguridad	✗	✓
Eficacia operacional	✓	✓

Modelo de Servicio Field Services 2.0 Grupo BeIT

Field Services 2.0 de GrupoBeIT representa un avance significativo en la gestión de servicios en campo, combinando tecnología avanzada, prácticas de seguridad robustas, y una gestión eficiente de recursos humanos y tecnológicos. Este modelo integral promete mejorar la calidad del servicio y la satisfacción del cliente. La implementación de estos pilares no solo protege a la organización de riesgos potenciales, sino que también optimiza la eficiencia operativa y fortalece la confianza de los clientes y socios.

> *A medida que los usuarios siguen trabajando desde cualquier lugar y los dispositivos IoT saturan las redes y los entornos operativos, es necesario realizar una verificación continua de todos los usuarios y dispositivos cuando acceden a las aplicaciones y los datos corporativos.*
>
> **Fortinet**

Edición #28

NEWSLETTER BeIT

El panorama de la seguridad Zero Trust está experimentando una transformación fundamental con la rápida adopción de estrategias basadas en la nube e iniciativas de transformación digital. Según el informe State of Zero Trust Transformation 2023 de Zscaler, aproximadamente el 90% de las empresas que migran a la nube están adoptando principios de seguridad Zero Trust. Este cambio es notable en el sector financiero, donde se priorizan las medidas de seguridad mientras se mejora la experiencia del cliente. Las arquitecturas de seguridad empresarial están evolucionando para abordar las complejidades de los entornos multinube y las fuerzas de trabajo distribuidas. Según el Informe State of Zero Trust 2023 de Fortinet, el 66% de las empresas encuestadas están utilizando soluciones de confianza cero para minimizar los impactos de las infracciones, un aumento significativo respecto a años anteriores.

GrupoBeIT ofrece soluciones avanzadas de Zero Trust Network Access (ZTNA), diseñadas para proporcionar un control de acceso detallado y seguro basado en la identidad y el perfil del usuario. Estas soluciones aseguran que ninguna entidad, ya sea interna o externa, sea de confianza por defecto. En lugar de otorgar acceso amplio a la red, el ZTNA de GrupoBeIT verifica continuamente la identidad y el contexto de los usuarios y dispositivos, permitiendo solo el acceso necesario para realizar tareas específicas. Las características destacadas de las soluciones ZTNA de GrupoBeIT incluyen, acceso mínimo necesario, protección de recursos en múltiples ubicaciones, y control de acceso adaptativo según el rol del usuario y el estado del dispositivo. Estas soluciones están diseñadas para mejorar la seguridad y la eficiencia operativa, protegiendo tanto los activos digitales como los datos sensibles de las organizaciones.

El mercado de control de acceso está experimentando un crecimiento notable. En 2024, se estimó que el tamaño del mercado alcanzaría los 3.52 mil millones de dólares y se espera que crezca a una tasa compuesta anual del 8.09%, llegando a 5.20 mil millones de dólares en 2029. Este crecimiento significativo se debe a varios factores clave.

1. **Tecnología Biométrica:** La creciente disponibilidad y adopción de equipos biométricos, especialmente el reconocimiento de huellas dactilares, está impulsando el mercado. Estos sistemas son rentables y ampliamente utilizados, mejorando la seguridad y la eficiencia.
2. **Interconexión de Dispositivos:** La creciente interconexión de dispositivos y los riesgos de seguridad asociados están fomentando la adopción de soluciones avanzadas de control de acceso. El Internet de las Cosas (IoT) juega un papel crucial en la automatización y eficiencia de estos sistemas, permitiendo el intercambio seguro de datos y la conexión de objetos inteligentes a Internet.
3. **Comunicación Basada en la Nube:** La comunicación en la nube ha facilitado el monitoreo remoto de áreas críticas y la autenticación de contraseñas para proteger los sistemas de seguridad basados en IoT. Esto ha llevado a la adopción de soluciones IoT en diversas aplicaciones, como sistemas de alarma inteligentes y abridores de puertas de garaje, reemplazando procesos tradicionales.

La integración de controles de acceso físicos a recursos (Sistemas de control de acceso) y digitales (ZTNA) ha aportado importantes beneficios. Estos sistemas y soluciones ahora funcionan de manera conjunta, proporcionando credenciales convergentes a los usuarios, reduciendo el riesgo de pérdida de credenciales y eliminando la necesidad de contraseñas complejas. Esta integración mejora la seguridad y la eficiencia operativa. A pesar de los beneficios, existen desafíos que pueden disuadir la adopción.

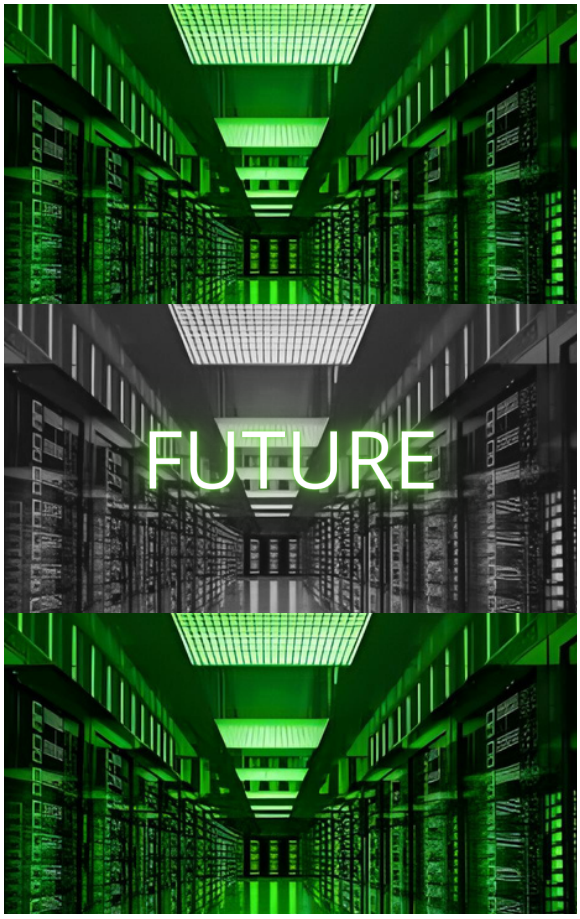
El control de acceso se ha convertido en la opción preferida para gestionar el acceso a edificios comerciales, oficinas, empresas e información. Ofreciendo una mayor seguridad para el acceso a recursos tanto físico como digitales. Un problema significativo que impulsa la demanda de estos sistemas y soluciones es el robo de empleados (robo de información, robo bienes físico, fraudes financieros). **Mordor Intelligence** hace mención al artículo de CompareCamp, donde detalla que las pérdidas globales por fraude y robo de empleados se estiman en 2.9 billones de dólares al año, y ser la responsable del 33% de las quiebras corporativas en los Estados Unidos. La implementación de sistemas y soluciones de control de acceso puede reducir efectivamente este tipo de eventos al permitir o denegar el acceso a áreas físicas críticas o a información confidencial.

Aunque los sistemas de control de acceso y el Zero Trust Network Access (ZTNA) comparten un bien común, el cual es proteger los recursos físicos y digitales de una organización mediante la gestión y restricción del acceso. Cada uno aborda desde una perspectiva y nivel de la infraestructura de seguridad.

Palo Alto hace referencia que los sistemas de control de acceso se centran en la gestión del acceso físico y lógico a recursos específicos dentro de una organización. Utilizan diversos métodos de autenticación, como tarjetas inteligentes, biometría y credenciales de proximidad, para permitir o denegar el acceso a áreas físicas o sistemas informáticos. Estos sistemas son esenciales para proteger áreas críticas y restringir el acceso a información confidencial. Mientras que ZTNA se enfoca en la seguridad de la red y el acceso a aplicaciones y servicios mediante un enfoque de "confianza cero". Este modelo asume que ninguna entidad, ya sea interna o externa, es de confianza por defecto. En lugar de otorgar acceso amplio a la red, el ZTNA verifica continuamente la identidad y el contexto de los usuarios y dispositivos, permitiendo solo el acceso necesario para realizar tareas específicas. Esto se logra mediante políticas de control de acceso detalladas y autenticación continua.

EVENTOS BeIT

ELIT
INFRASTRUCTURE
SERVICES



Schneider Electric

El próximos 23 y 24 de abril, nuestro equipo de Elit Infrastructure Services participará en una certificación especializada con nuestro socio Schneider Electric, a través de su programa de capacitaciones. Esta certificación en Cooling para diversos entornos nos permitirá seguir ofreciendo la mejor tecnología y mejor dimensionamiento a nuestros clientes basados en sus necesidades.

Como Grupo BeIT, seguimos comprometidos con nuestros clientes y colaboradores. Nos enorgullecen los logros alcanzados y estamos seguros de que esta formación contribuirá significativamente a brindar una mejor atención y soporte a nuestros clientes.

Seguridad en Redes 5G

Procesamiento, Almacenamiento, Respaldos, Redes, Consumo

Las redes 5G presentan desafíos significativos en términos de seguridad debido a su arquitectura más compleja y distribuida. Los riesgos potenciales incluyen vulnerabilidades en la cadena de suministro, ataques de phishing, ataques DDoS (denegación de servicio distribuido) y amenazas a dispositivos IoT. La implementación de medidas de seguridad avanzadas, como la segmentación de red y la computación perimetral, es crucial para minimizar estas vulnerabilidades.

Huawei destaca la importancia de la ciberseguridad en las redes 5G y ha promovido la colaboración con la industria para establecer estándares comunes de seguridad. Según Huawei, los riesgos de seguridad en las redes 5G pueden gestionarse de manera efectiva mediante protocolos y estándares de seguridad, así como mecanismos que garanticen la confidencialidad, integridad de la información de los usuarios y la disponibilidad del servicio