Grupo BeIT

Blog CEO

Ciberseguridad , esencial en tecnologías operativas (OT) y tecnologías de la información (IT)

Noticia BeIT

La Corte Penal Internacional sufre un nuevo y sofisticado ciberataque

Edición 39º

Estado de la tecnología operativa y la ciberseguridad

Partners BeIT

TechDay Huawei

TechDay Field Services 2.0

19 AÑOS

ELIT INFRASTRUCTURE SERVICES

BURÓMC SEGURIDAD INFORMÁTICA

Este mes de julio celebramos con orgullo 19 años de crecimiento y desarrollo continuo, no solo como proveedores de soluciones tecnológicas, sino como aliados estratégicos en cada etapa de nuestros clientes y socios. Desde la estrategia hasta la operación, todo ello bajo marcos de normativas internacionales de ciberseguridad e infraestructuras robustas, como son la ISO 20000 , ISO 27001 e IEC 62443.

Nuestra historia la hemos podido cambiar con una visión clara, con un equipo apasionado, y con una cultura centrada en la excelencia. La cercanía y la mejora constante en cada área de GrupoBelT y sus empresas adjuntas, desde la preventa hasta la operación, trabajan con un mismo propósito: generar valor real y sostenible en el tiempo.

En estos 19 años, aprendimos, innovamos y evolucionamos. Hemos transitado con éxito y sin duda alguna con aprendizaje, desde de las tecnologías. Field Services 2.0 de GrupoBelT nos brinda eso, una postura segura y alineada con los desafíos actuales de la industria, la misma que necesita tener seguridad, disponibilidad, eficiencia, resiliencia, homologación y continuidad operativa.

Este camino ha sido posible gracias a un equipo técnico y administrativo de primer nivel, con procesos centrados en la experiencia del cliente y una mentalidad de innovación constante. Que hoy en día, nos permite tener presencia a nivel nacional con más de 200 técnicos, brindando servicio y soluciones llave en mano, ayudando a que nuestros clientes alcancen sus objetivos.

Gracias por ser parte de esta historia. Y lo mejor ¡ya lo estamos construyendo juntos!

José Luis Coronado
GrupoBelT
Director de Preventa y Cuentas Esttratégicas

Ciberseguridad , esencial en tecnologías operativas (OT) y tecnologías de la información (IT)

Por: Elías Cedillo , Fundador y *CEO GrupoBeIT*

La convergencia entre la tecnología operativa (OT) y la tecnología de la información (IT) se ha convertido en una estrategia clave para proteger infraestructuras críticas en sectores como energía, manufactura, petróleo y gas, telecomunicaciones, robótica, tratamiento de residuos y gestión del agua. Esta integración no solo representa una evolución tecnológica, sino una respuesta necesaria ante los crecientes desafíos de ciberseguridad en entornos industriales cada vez más conectados.

La OT se enfoca en el control y automatización de procesos industriales mediante hardware y software especializados. Su objetivo principal es garantizar la continuidad operativa y la precisión en sistemas donde cualquier interrupción puede tener consecuencias graves. Entre sus componentes destacan los Sistemas de Control Industrial (ICS), como SCADA (Supervisory Control and Data Acquisition), que recopilan y analizan datos en tiempo real, y los Controladores Lógicos Programables (PLC), que automatizan tareas críticas como el monitoreo de variables y la ejecución de procesos complejos.

A diferencia de la IT, los sistemas OT suelen operar con software propio, configuraciones personalizadas y ciclos de actualización limitados, debido al impacto que puede tener detener procesos industriales. Tradicionalmente, estos sistemas estaban aislados de redes externas, lo que limitaba su exposición a amenazas. Sin embargo, la digitalización ha impulsado su conectividad, mejorando la eficiencia operativa, pero también ampliando la superficie de ataque.

Por su parte, la IT se encarga del desarrollo, mantenimiento y administración de sistemas informáticos, redes y software. Sus funciones abarcan operaciones diarias, infraestructura tecnológica y gobernanza, con un enfoque en la protección de datos, dispositivos y servicios digitales mediante herramientas como antivirus, firewalls y protocolos estándar.

La creciente interconexión entre OT e IT ha generado nuevas vulnerabilidades que pueden ser explotadas por actores maliciosos. Según el Ponemon Institute, más del 90 % de las organizaciones con sistemas OT han sufrido al menos un incidente de seguridad en los últimos dos años, y la mitad de ellas reportaron interrupciones operativas como consecuencia directa.

Frente a este panorama, es indispensable adoptar un enfoque integral de ciberseguridad que contemple las particularidades de ambos entornos. Soluciones como los sistemas de gestión de eventos e información de seguridad (SIEM) y los firewalls de próxima generación (NGFW) permiten monitorear y proteger redes híbridas de forma más eficaz.

Además, la colaboración entre los equipos de seguridad de IT y OT se vuelve esencial para garantizar la continuidad operativa, la resiliencia ante amenazas y la sostenibilidad de los procesos críticos. Solo mediante una estrategia unificada será posible proteger eficazmente tanto los activos digitales como los industriales en un mundo cada vez más interconectado.

Tradicionalmente, los sistemas OT estaban aislados de redes públicas e internas, lo que limitaba su exposición a amenazas externas. Sin embargo, la digitalización ha permitido que estos sistemas sean monitoreados y controlados remotamente, lo que mejora la eficiencia operativa, pero también incrementa los riesgos de ciberseguridad.

A medida que más organizaciones conectan sus sistemas OT para mejorar la productividad y la seguridad, la colaboración entre los equipos de seguridad de IT y OT se vuelve indispensable. La falta de medidas de protección adecuadas en OT, combinada con el aumento de la conectividad, incrementa la exposición a amenazas cada vez más sofisticadas.

En conclusión, la IT y OT exige una visión unificada de la ciberseguridad. Sólo mediante una estrategia integral, que contemple las particularidades de ambos entornos, será posible proteger eficazmente las infraestructuras críticas y garantizar la continuidad de las operaciones en un mundo cada vez más interconectado.

Referencia:
Fortinet

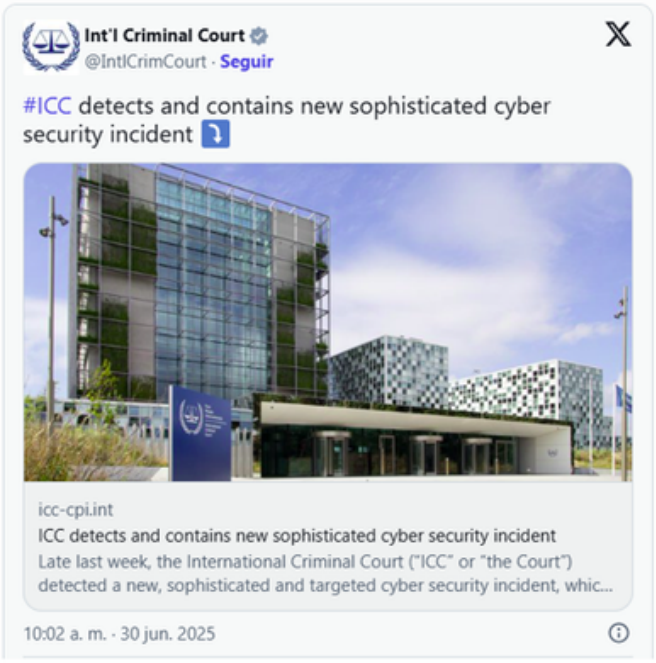
NOTICIA BeIT

Panorama Global

La Corte Penal Internacional sufre un nuevo y sofisticado ciberataque

El pasado 30 de junio del 2025 La Corte Penal Internacional (CPI) informó que logró contener un ciberataque altamente sofisticado que afectó sus sistemas. El incidente fue detectado de manera oportuna gracias a los mecanismos de alerta y respuesta del tribunal, lo que permitió una rápida intervención para mitigar sus posibles consecuencias.

En un comunicado oficial, la CPI explicó que el ataque fue “nuevo, sofisticado y específico”, y que ya se encuentra bajo control. Aunque no se han revelado detalles sobre los autores del ataque ni sobre la posible exposición de datos sensibles, el tribunal aseguró que se están llevando a cabo análisis exhaustivos para evaluar el impacto del incidente y reforzar sus medidas de seguridad.



Este evento representa el segundo ciberataque significativo que enfrenta la Corte en los últimos años, luego del registrado en septiembre de 2023. La recurrencia de estos ataques subraya la creciente amenaza que enfrentan las instituciones internacionales en el ámbito digital, especialmente aquellas que manejan información sensible relacionada con crímenes de guerra, lesa humanidad y genocidio.

La sede de la CPI, ubicada en La Haya, ha reiterado su compromiso con la protección de sus sistemas y la integridad de sus procesos judiciales. Aunque el comunicado no ofreció detalles técnicos sobre el ataque, sí destacó la eficacia de sus protocolos de ciberseguridad para contener la amenaza de forma inmediata.
Este incidente pone de relieve la importancia de fortalecer las infraestructuras digitales de organismos internacionales, en un contexto global donde los ciberataques se han convertido en herramientas frecuentes de presión y desestabilización.

Referencia:
Forbes México

BURŌMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

Edición 39°

NEWSLETTER BeIT

Estado de la tecnología operativa y la ciberseguridad

En el contexto actual y la creciente interconectividad, la seguridad de la tecnología operativa (OT) se ha convertido en un pilar esencial para garantizar la continuidad, integridad y resiliencia de las operaciones industriales y de infraestructura crítica. A diferencia de los entornos de tecnología de la información (IT), los sistemas OT presentan desafíos únicos que exigen un enfoque especializado en ciberseguridad.

Los sistemas OT están diseñados para operar de forma continua, con altos niveles de disponibilidad que limitan las oportunidades para mantenimiento o actualizaciones. Esta característica, aunque fundamental para la eficiencia operativa, los convierte en blancos atractivos para ciberataques como malware, ransomware y amenazas persistentes avanzadas. Además, muchos de estos sistemas utilizan protocolos heredados y propietarios, lo que dificulta su integración con soluciones de seguridad convencionales.

La convergencia entre IT y OT, impulsada por tecnologías como el Internet de las Cosas (IoT), el Internet Industrial de las Cosas (IIoT) y la digitalización de procesos, ha ampliado significativamente la superficie de ataque. Lo que antes eran entornos aislados, ahora están expuestos a riesgos complejos que requieren una postura de seguridad integral y coordinada.

Para mitigar estos riesgos, las organizaciones deben adoptar un enfoque holístico que combine tecnología avanzada, procesos robustos y colaboración interdepartamental. Algunas prácticas recomendadas incluyen:

- Segmentación de redes para aislar sistemas críticos y evitar la propagación de amenazas.
- Firewalls de próxima generación (NGFW) y puertas de enlace unidireccionales, que permiten comunicaciones seguras sin comprometer la integridad del sistema.
- Sistemas SIEM e IAM, que facilitan el monitoreo, la detección y la respuesta a amenazas en tiempo real.
- Evaluaciones periódicas de riesgos, gestión de vulnerabilidades y planes de respuesta a incidentes bien definidos.

La colaboración entre los equipos de IT y OT, así como con proveedores externos de ciberseguridad, es fundamental para lograr una defensa coordinada y una visibilidad completa del ecosistema.

El modelo de seguridad Zero Trust se posiciona como una estrategia clave para proteger entornos OT. Este enfoque parte del principio de que ningún dispositivo, usuario o aplicación debe ser confiado por defecto, independientemente de su ubicación. Cada intento de acceso debe ser autenticado, autorizado y monitoreado de forma continua
.
Como señala Dave Gruber, analista de Enterprise Strategy Group:

“A medida que aumenta la interconexión entre los sistemas de OT e IT, también lo hace la superficie de ataque. Defenderse de amenazas sofisticadas requiere estrategias de seguridad más amplias, con visibilidad, contexto detallado y funciones de Confianza Cero para todos los dispositivos, redes, aplicaciones y usuarios.”

Este modelo permite proteger cargas de trabajo en la nube, dispositivos OT, nodos de red y usuarios, garantizando una postura de seguridad coherente y adaptable.

Un ataque exitoso a sistemas OT puede tener consecuencias devastadoras: interrupciones operativas, pérdidas económicas, daños físicos, riesgos ambientales y sanciones regulatorias. Según el Institution of Mechanical Engineers (IMechE), el costo promedio de un paro no programado en una fábrica puede oscilar entre 1,200 y 58,800 USD por minuto, dependiendo del sector y la escala de operación.

Por ejemplo, una fábrica de componentes electrónicos con una producción diaria de 1,000 unidades a un valor de 117.54 USD por unidad podría perder más de 235,000 USD en ingresos por solo dos horas de inactividad.

La evolución de los entornos industriales exige una transformación en la forma de abordar la ciberseguridad. La separación tradicional entre redes IT y OT ha demostrado ser ineficiente, generando duplicidad de esfuerzos y falta de visibilidad. Superar estas limitaciones requiere soluciones integradas que permitan una gestión centralizada y una respuesta coordinada ante incidentes.

Gartner define la seguridad OT como:

“Prácticas y tecnologías utilizadas para proteger personas, activos e información, monitorear o controlar dispositivos físicos, procesos y eventos, e iniciar cambios de estado en los sistemas OT empresariales.”

Esta definición subraya la necesidad de un enfoque estratégico que combine tecnología, procesos y personas para proteger los activos más críticos de la organización.

La seguridad de OT no es negociable. Su vulneración puede afectar servicios esenciales como plantas de tratamiento de agua, sistemas de tráfico o servicios de emergencia, con consecuencias que van desde pérdidas económicas hasta la pérdida de vidas humanas. Incluso sectores no considerados como infraestructura crítica, como la industria alimentaria, pueden enfrentar riesgos graves si se comprometen los controles de seguridad.

Los cibercriminales han ampliado su enfoque hacia redes OT, conscientes de su valor estratégico y de las brechas de seguridad existentes. Según el Informe de Estado de Tecnología Operativa de Fortinet, casi el 74 % de las organizaciones OT reportaron intrusiones de malware en los últimos 12 meses, afectando productividad, ingresos, propiedad intelectual y seguridad física.

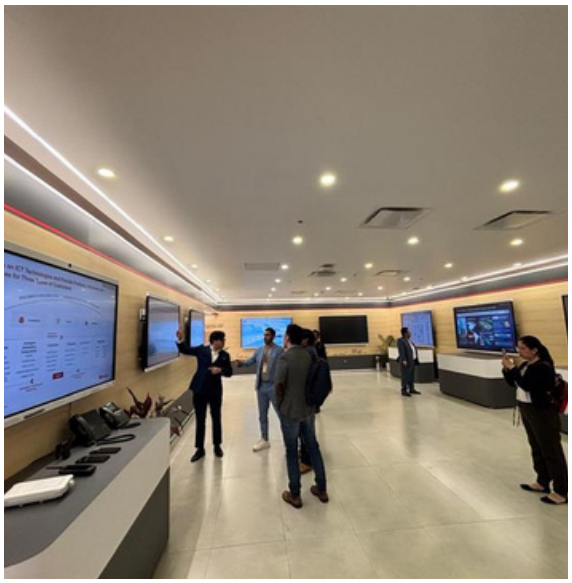
Referencias:

Fortinet
IBM
Palo Alto
Rosmiman
Gartner

¡Gracias Huawei Enterprise por la invitación

El 9 de julio tuvimos el privilegio de visitar el Demo Room de nuestro partner estratégico Huawei Latinoamérica, un espacio diseñado para experimentar de primera mano el alcance y la innovación de sus soluciones tecnológicas aplicadas a diversos sectores.

La visita fue una experiencia enriquecedora que nos permitió conocer en profundidad sus propuestas, intercambiar ideas valiosas y explorar nuevas oportunidades de colaboración entre nuestros equipos.
Nos llevamos inspiración, aprendizajes y una renovada motivación para seguir construyendo juntos un futuro más conectado, eficiente e innovador. 💡🤝



Elías Cedillo
GrupoBeIT
Fundador y Director General

vicarius netskope PARTNERS BeIT

FIELD SERVICES 2.0

Servicio técnico especializado en ciberseguridad los 365 días del año

Grupo BeIT junto a Vicarius y Netskope te invitan este **21 de agosto** a vivir la evolución de los servicios en campo en nuestro evento exclusivo **Field Services 2.0**, donde presentaremos cómo nuestro modelo transforma la operación tradicional mediante tecnología en la nube, soporte remoto, mantenimiento predictivo y un enfoque de ciberseguridad basado en Zero Trust; todo impulsado por ingenieros especializados y una **visión proactiva que optimiza costos, tiempos y seguridad**. Acompáñanos para descubrir cómo esta propuesta está revolucionando sectores como Food & Beverage, Salud, Banca y Finanzas, entre otras.

¡No te lo pierdas!

Escríbenos
y aparta tu lugar

ó

Da clic o escanea el QR
y aparta tu lugar