Grupo BeIT

NEWSLETTER

Blog CEO

Ethical Hacking
solución a la medida

Noticia BeIT

Jaguar Land Rover reinicia la producción, más de un mes después del ciberataque sufrido a finales de agosto.

Edición 46

¿Cómo las empresas mexicanas pueden sobrevivir en un entorno de 35 mil millones de ciberataques y riesgos de IA sin gobernanza?

Eventos

Webinars: Defensa Industrial: La Ciberseguridad en entornos Operational Technology (OT) al descubierto

Edición 46

ELIT INFRASTRUCTURE SERVICES

BURÓMC SEGURIDAD INFORMÁTICA

Ethical Hacking solución a la medida

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

BM define al Ethical Hacking como la práctica mediante la cual profesionales utilizamos técnicas de hacking para poder identificar, comprender y corregir vulnerabilidades en redes, sistemas informáticos y aplicaciones, sin causar daño alguno, sino poder brindar un mejor dimensionamiento del estado actual de las organizaciones en carácter de seguridad digital. Se emplean las mismas herramientas, tácticas y habilidades que los atacantes maliciosos, pero con el objetivo de fortalecer la seguridad de una organización. Es, en esencia, un ensayo controlado de ciberataques reales, que permite a las empresas anticiparse a amenazas, mejorar sus defensas y proteger sus datos confidenciales.

GrupoBeIT, en el entorno donde la ciberseguridad se ha convertido en un pilar estratégico para la continuidad operativa y la reputación corporativa, se posiciona como un aliado clave para las organizaciones que buscan soluciones de protección avanzadas y adaptadas a su realidad tecnológica. Por ello, en la actualidad ofrece servicios de Ethical Hacking Modular, diseñados a la medida, que permiten identificar vulnerabilidades críticas, simular ataques reales y anticiparse a amenazas emergentes. Su enfoque modular responde a los desafíos actuales del entorno digital, habilitando a los líderes empresariales a tomar decisiones informadas, seguras y alineadas con sus objetivos de negocio.

La propuesta modular de GrupoBeIT se estructura en cinco ejes fundamentales que pueden implementarse de forma independiente o como parte de una estrategia integral: análisis de vulnerabilidades, pruebas de penetración (pentesting), análisis de código fuente, evaluación de rendimiento y monitoreo de amenazas en la dark web y deep web.
El análisis de vulnerabilidades permite identificar debilidades en sistemas, aplicaciones y configuraciones antes de que sean explotadas. Esta práctica se basa en estándares internacionales como OWASP, NIST y ISO/IEC 27001, y se complementa con escaneos automatizados y revisiones manuales. El objetivo es reducir la superficie de ataque y anticiparse a incidentes que puedan comprometer la operación o la reputación corporativa.

Las **pruebas de penetración** simulan ataques reales para evaluar la resistencia de los sistemas ante amenazas internas y externas. En GrupoBeIT aplicamos herramientas especializadas para replicar escenarios de ataque, incluyendo acceso no autorizado, escalamiento de privilegios y exfiltración de datos. Este servicio es especialmente útil en sectores como banca, salud, servicios financieros/profesionales, manufactura, retail, entre otros, donde la disponibilidad y la integridad de los sistemas son esenciales.

El análisis de código fuente se enfoca en detectar vulnerabilidades desde la etapa de desarrollo. Mediante revisiones estáticas y dinámicas, se identifican errores de lógica, malas prácticas de programación y riesgos de seguridad que podrían ser explotados en producción. Esta práctica es clave para organizaciones que operan bajo modelos DevSecOps, ya que permite integrar la seguridad en el ciclo de vida del software.

La evaluación de rendimiento analiza cómo los sistemas responden bajo condiciones de estrés, carga elevada o ataques de denegación de servicio. GrupoBeIT realiza pruebas de carga y escalabilidad para identificar cuellos de botella y optimizar la infraestructura tecnológica. Esta evaluación es crítica para empresas con alta transaccionalidad digital, donde la experiencia del usuario y la continuidad operativa son factores de competitividad.

El monitoreo de la dark web y deep web proporciona inteligencia anticipada sobre amenazas emergentes. A través del Security Operations Center (SOC) rastreamos foros clandestinos, mercados ilegales y redes de intercambio de información maliciosa, detectando credenciales comprometidas, filtraciones de datos y campañas de ataque en preparación. Esta observabilidad permite activar alertas tempranas y tomar medidas preventivas antes de que los incidentes se materialicen.

La modularidad de esta solución permite a los líderes empresariales diseñar esquemas de seguridad adaptados a su realidad operativa, presupuesto y nivel de exposición. GrupoBeIT como un aliado estratégico para sus clientes en cada etapa del proceso, desde el diagnóstico inicial hasta la implementación y monitoreo continuo, integrando consultoría especializada, tecnología de vanguardia y soporte técnico.

En un contexto donde México ha registrado más de 35 mil millones de intentos de ciberataques en el primer trimestre de 2025, y donde las organizaciones enfrentan un promedio de 3,048 ataques semanales, adoptar soluciones de Ethical Hacking a la medida no es una opción, sino una necesidad estratégica. GrupoBeIT ofrece una respuesta sólida, escalable y alineada con los desafíos actuales, permitiendo a las empresas operar con seguridad, eficiencia y visión de futuro.

Panorama Global

Jaguar Land Rover reinicia la producción, más de un mes después del ciberataque sufrido a finales de agosto.

NOTICIA BeIT

Jaguar Land Rover se convirtió en el epicentro de uno de los ciberataques más disruptivos en la industria automotriz moderna. El incidente, atribuido al grupo Scattered Lapsus$ Hunters, paralizó la producción global de la compañía durante más de cinco semanas y puso en evidencia la fragilidad de las cadenas de suministro frente a amenazas digitales. Todo comenzó el 31 de agosto, cuando se detectó una intrusión que afectó sistemas críticos y obligó a detener la fabricación el 1 de septiembre. Desde ese momento, las plantas en el Reino Unido, Eslovaquia, India y Brasil quedaron inoperativas, y los concesionarios tuvieron que recurrir a procesos manuales para mantener operaciones mínimas.

El impacto económico fue inmediato y profundo. Antes del ataque, Jaguar Land Rover producía cerca de mil vehículos diarios, pero la cifra cayó a cero, generando pérdidas estimadas en más de cincuenta millones de libras por semana, con cálculos alternativos que proyectaban hasta ochenta y dos millones de euros diarios. Ante el riesgo de colapso en la cadena de suministro, el gobierno británico intervino con una garantía de préstamo por mil quinientos millones de libras, equivalente a unos dos mil millones de dólares, para sostener a proveedores estratégicos y evitar un efecto dominó que amenazaba más de ciento cincuenta mil empleos indirectos. Esta respuesta estatal subraya que un ciberataque a un fabricante ancla únicamente no es un problema corporativo, sino un riesgo sistémico con implicaciones macroeconómicas.

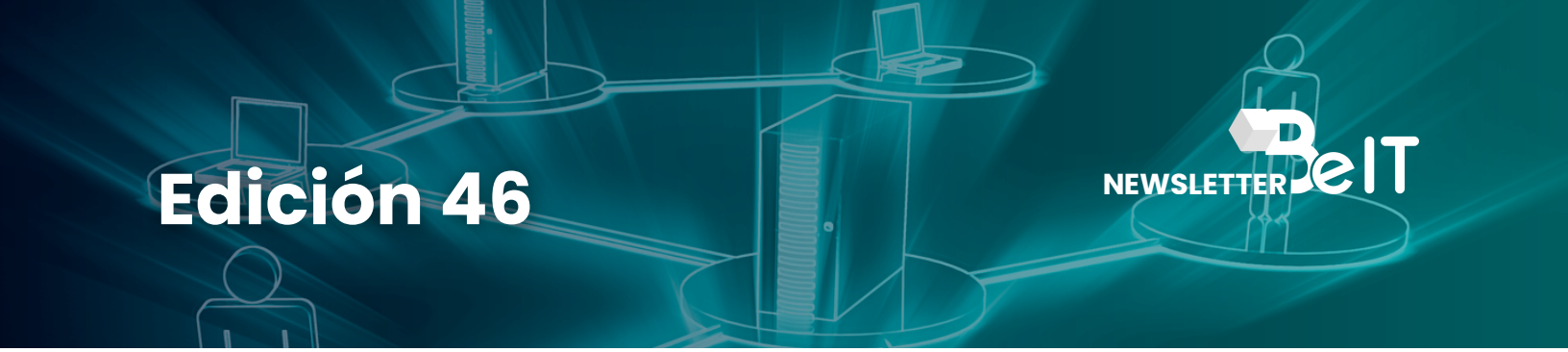
En paralelo, la compañía enfrentó un desafío reputacional y regulatorio. Inicialmente negó la filtración de datos, pero posteriormente admitió que cierta información se había visto comprometida, notificando a las autoridades competentes. Aunque no se ha confirmado el alcance exacto, expertos sugieren que podrían haberse expuesto datos de clientes, proveedores y diseños internos. El vector de ataque apunta a la explotación de una vulnerabilidad en SAP NetWeaver, lo que revela una dependencia crítica de sistemas ERP y la necesidad urgente de reforzar controles en software empresarial y accesos privilegiados.

Las consecuencias estratégicas no se limitan al corto plazo. El parón obligó a retrasar lanzamientos clave, incluyendo el modelo eléctrico Type 00 y versiones sin motor de combustión de Range Rover, Velar y Defender, afectando la narrativa de transformación hacia la movilidad eléctrica. Además, la falta de seguro contra ciberataques amplificó el impacto financiero, dejando a la empresa expuesta a pérdidas directas y a una presión adicional sobre márgenes y liquidez. Este escenario plantea preguntas esenciales para cualquier comité ejecutivo: ¿cómo segmentar efectivamente entornos IT y OT?, ¿qué mecanismos de autenticación y control de privilegios son resistentes a ataques sofisticados?, ¿cómo blindar la relación con terceros y garantizar parches críticos en tiempo real?, y ¿qué estrategias de transferencia de riesgo son indispensables para mitigar impactos de esta magnitud?

La reanudación de operaciones comenzó el 8 de octubre, de manera gradual y controlada, priorizando nodos críticos como motores, baterías y estampado, para recuperar el flujo mínimo de producción. Sin embargo, el caso Jaguar Land Rover deja una lección clara: la ciberseguridad ya no es un tema técnico aislado, sino un factor determinante para la continuidad del negocio, la estabilidad sectorial y la confianza del mercado. En un entorno donde la digitalización permea cada eslabón de la cadena industrial, la resiliencia se convierte en la nueva eficiencia. Las organizaciones que no integren la ciberprotección en su estrategia corporativa estarán expuestas a interrupciones operativas, así como a crisis financieras y reputacionales que pueden redefinir su posición competitiva en cuestión de días.

Referencias

- The Independent
- PCMag
- Yahoo/AFP
- USA Today
- Xataka
- La Vanguardia
- Autonocion
- Carscoops
- Diariomotor
- The Objective
- InsuranceJournal



Edición 46

NEWSLETTER BeIT

¿Cómo las empresas mexicanas pueden sobrevivir en un entorno de 35 mil millones de ciberataques y riesgos de IA sin gobernanza?

El Ethical Hacking ha evolucionado de ser una práctica técnica puntual a convertirse en un componente esencial de la estrategia empresarial moderna. En un entorno donde las amenazas digitales se multiplican y sofistican, los líderes C-Level enfrentan el reto de proteger los activos, la reputación y la continuidad operativa de sus organizaciones. La simulación controlada de ataques cibernéticos por parte de profesionales autorizados permite identificar vulnerabilidades antes de que sean explotadas por actores maliciosos. IBM lo define como un ensayo técnico de ataques reales que fortalece las defensas sin causar daño, operando bajo principios de legalidad, confidencialidad y ética profesional.

Los beneficios del Ethical Hacking son claros y estratégicos. IBM destaca su capacidad para identificar proactivamente vulnerabilidades, simular ataques reales y realizar evaluaciones de malware y pruebas de penetración. Fortinet, por su parte, subraya su papel en la defensa contra ataques automatizados, el robo de credenciales y la explotación de configuraciones débiles en la nube, así como en la prevención frente al uso de inteligencia artificial maliciosa como FraudGPT y BlackmailerV3. Dell complementa esta visión al posicionar la ética y la confianza como pilares fundamentales de la ciberseguridad empresarial, promoviendo prácticas responsables y transparentes que refuerzan la reputación corporativa y la continuidad operativa.

El panorama mexicano exige atención inmediata. Según el informe “Panorama Global de Amenazas 2025” de Fortinet, México registró más de 35,200 millones de intentos de ciberataques solo en el primer trimestre del año, posicionándose como el segundo país más atacado en América Latina, únicamente detrás de Brasil. Esta cifra refleja un incremento sostenido respecto a años anteriores y evidencia la creciente sofisticación de las amenazas digitales que enfrentan empresas, instituciones gubernamentales y usuarios particulares. Además, el Threat Intelligence Report de Check Point reveló que las organizaciones mexicanas reciben en promedio 3,048 ataques semanales, muy por encima del promedio global de 1,891. Esta sobreexposición convierte a México en un blanco prioritario para los ciberdelincuentes, quienes aprovechan la cercanía geográfica con Estados Unidos y la creciente digitalización del país.

La situación es aún más crítica para las pequeñas y medianas empresas. De acuerdo con Alejandra Lagunes, fundadora de la Alianza Nacional de Inteligencia Artificial (ANIA), siete de cada diez pymes que sufren un ciberataque en México terminan en quiebra. Esta alarmante estadística se explica por la falta de protección robusta, la escasa inversión en seguridad digital y los elevados costos financieros que implica la recuperación de datos y la restauración de operaciones. En muchos casos, las pymes no cuentan con planes de contingencia ni personal especializado, lo que las convierte en blancos fáciles para los ciberdelincuentes. La prevención, en este contexto, no es una opción: es una necesidad estratégica.

El informe "Cost of a Data Breach 2025", elaborado por IBM en colaboración con el Instituto Ponemon, ofrece una perspectiva histórica y actualizada sobre la evolución de las amenazas. Hace dos décadas, casi la mitad de las filtraciones de datos eran causadas por la pérdida o el robo de dispositivos físicos, mientras que solo una décima parte se atribuía a sistemas comprometidos. Hoy, la mayoría de los incidentes se originan en actividades maliciosas como el phishing, el abuso de credenciales y las amenazas internas. Hace apenas diez años, las filtraciones por mala configuración en la nube ni siquiera se consideraban una categoría de riesgo. Hoy, la nube y los datos que contiene son un objetivo principal. Durante los confinamientos por COVID-19 en 2020, el ransomware comenzó a escalar, y un año después, estos ataques representaban un promedio de 4.62 millones de dólares en costos por filtración, cifra que alcanzó los 5.08 millones de dólares en el informe de este año.

El costo promedio global de una filtración de datos en 2025 se ubicó en 4.44 millones de dólares, lo que representa una reducción del 9% respecto al año anterior. Esta disminución se atribuye a mejoras en la velocidad de detección y contención de incidentes. Las organizaciones que han adoptado ampliamente inteligencia artificial y automatización en sus operaciones de seguridad lograron ahorros promedio de 1.9 millones de dólares por incidente, además de reducir el ciclo de vida de la filtración en 80 días. Estos resultados confirman el valor de la IA como herramienta defensiva.

Sin embargo, el uso de IA también conlleva riesgos. El 13% de las organizaciones reportaron brechas en modelos o aplicaciones de inteligencia artificial. De estas, el 97% no contaban con controles de acceso adecuados, lo que derivó en que el 60% de los incidentes relacionados con IA comprometieran datos sensibles, y el 31% provocaran interrupciones operativas. A pesar de estos riesgos, el 63% de las organizaciones afectadas no tienen una política formal de gobernanza de IA o están en proceso de desarrollarla. Solo el 34% realiza auditorías regulares para detectar el uso no autorizado de IA, fenómeno conocido como "Shadow AI".

Ante este panorama, IBM recomienda implementar controles operativos sólidos para identidades no humanas (NHIs), adoptar métodos modernos de autenticación resistentes al phishing, como las passkeys, y fortalecer la observabilidad de los sistemas de IA. La clasificación de datos sensibles también se vuelve esencial para detectar anomalías y mejorar el cumplimiento normativo. El informe enfatiza la importancia de probar regularmente los planes de respuesta a incidentes, definir roles claros ante una brecha y realizar simulaciones de crisis para mejorar la resiliencia organizacional.

Gartner reconoce el Ethical Hacking como parte integral de una estrategia de gestión proactiva de exposición, destacando a Fortinet como líder en soluciones de firewall híbrido, SASE, SD-WAN y LAN empresarial. También, los usuarios valoran los servicios de hacking ético por su profundidad técnica y capacidad de integración con sistemas empresariales, según Gartner Peer Insights. Esta validación del mercado confirma que el Ethical Hacking es una práctica técnica, al mismo tiempo que una decisión estratégica que impacta directamente en la resiliencia organizacional.

Mordor Intelligence proyecta un crecimiento acelerado del mercado global de servicios de Ethical Hacking, pasando de USD 2.15 mil millones en 2025 a USD 5 mil millones en 2030, con una tasa compuesta anual del 18.37%. En México, se espera que el mercado de ciberseguridad alcance los USD 2.80 mil millones en 2025 y crezca hasta USD 4.85 mil millones en 2030. Esta evolución refleja una transición hacia servicios continuos integrados en entornos DevSecOps, lo que exige una visión estratégica y sostenida por parte del liderazgo empresarial.

En conclusión, el Ethical Hacking representa una transformación estratégica y necesaria para las organizaciones mexicanas que buscan proteger su operatividad, activos, reputación y cumplir con normativas internacionales. Grupo BelT con su conglomerado de empresas BuróMC Seguridad Informática y Elit Infrastructure Services están marcando el camino hacia una ciberseguridad e infraestructura más robusta, de la mano con información valiosa para sus clientes, usuarios y seguidores. Para los líderes de las organizaciones hemos preparado una campaña de Ethical Hacking Modular donde podrán acceder a una o varias soluciones que más se adapten a sus estrategias corporativas. El camino de negocio a seguir debe ayudar a la continuidad operativa, confianza del cliente y ventaja competitiva.

Referencias:

1. IBM – Cost of a Data Breach Report 2025
2. IBM Newsroom – IA y automatización en ciberseguridad
3. Fortinet – Panorama Global de Amenazas 2025
4. Check Point – Threat Intelligence Report 2025
5. ANIA – Alianza Nacional de Inteligencia Artificial:
6. Gartner
7. Dell Technologies – Cybersecurity Insights
8. Mordor Intelligence – Ethical Hacking Market Report

ELIT INFRASTRUCTURE SERVICES

Grupo BeIT

Serie de Webinars

Defensa Industrial: La Ciberseguridad en entornos Operational Technology (OT) al descubierto

Te invitamos a descubrir una serie de 3 episodios donde desciframos los retos, riesgos y soluciones del entorno en la seguridad industrial. Cada episodio aborda una etapa clave en el camino hacia un entorno OT seguro, resiliente y alineado con estándares internacionales, aunque puedes unirte al que más se ajuste a tu rol o interés.

Una producción de GrupoBeIT con sus marcas BuróMC Seguridad Informática y Elite Infrastructure Services para distintos niveles de decisión y operación, con un enfoque práctico y basado en escenarios reales.

EPISODIO 1: "Fundamentos de la Defensa OT"
Fecha: Martes, 14 de octubre
Hora: 11:00 hrs.

EPISODIO 2: "Evaluando el Riesgo: Diagnóstico y Madurez"
Fecha: Jueves, 30 de octubre
Hora: 16:00 hrs

EPISODIO 3: "Estrategias de Mitigación: Diseñando la Defensa OT"
Fecha: Jueves, 6 de noviembre
Hora: 11:00 hrs.

Registro

Contacto

+52 56 5100 8613

admmarketing@buromc.com