Grupo BeIT

19 AÑOS

NEWSLETTER

Blog CEO

Seguridad de aplicaciones web

Noticia BeIT

SHUYAL, el malware que rompe barreras y amenaza a 19 navegadores web.

Edición 41

Sistema de Gestión de la Ciberseguridad Industrial (SGCI)

Edición 41

ELIT INFRASTRUCTURE SERVICES

BURÖMC SEGURIDAD INFORMÁTICA

Celebramos XIX años de aprendizaje , innovación y evolución, con un equipo comprometido, desde sus procesos centrados a la mejor experiencia de nuestros clientes. GrupoBeIT, BuróMC Seguridad Informática y Elit Infrastructure Services mantienen una visión clara, una cercanía al desarrollo y una mejora constante en la innovación tecnológica e infraestructura, lo que ha permitido ejecutar proyectos de alto impacto en los diversos sectores industriales mexicanos.

Actualmente contamos con tecnologías cada vez más especializadas, diseñadas para responder con precisión a las necesidades de los diferentes sectores industriales del mercado mexicano. Gracias a la estrecha colaboración con nuestros partner, hemos logrado integrar soluciones que se adaptan a los requerimientos operativos de nuestros clientes, sino que también se incorporan de forma natural a sus procesos, potenciando su eficiencia, resiliencia y capacidad de innovación.

Esta sinergia ha permite ofrecer servicios y soluciones que acompañan a las empresas en su transición digital, sin comprometer la continuidad operativa ni la experiencia de sus usuarios. Trabajar de la mano con partners líderes en ciberseguridad IT y OT, infraestructura, energía y enfriamiento, nos brinda un portafolio robusto y flexible, capaz de responder a los desafíos actuales.

Nuestros partners aportan tecnología de vanguardia, también conocimiento profundo del mercado, visión estratégica y compromiso con la excelencia. Juntos, construimos un ecosistema colaborativo que impulsa a la transformación de las empresas mexicanas, fortaleciendo su competitividad y preparándolas para enfrentar con éxito los retos.

En GrupoBeIT y sus partners entendemos que la implementación tecnológica debe ir acompañada de una estrategia financiera y logística sólida. Por ello, procuramos siempre brindar la mejor opción que se alinee con los objetivos estratégicos del negocio de nuestros clientes y sea efectiva en todo nivel. Desde la planeación hasta la ejecución, nuestras propuestas están diseñadas para potenciar el crecimiento, optimizar recursos y asegurar que cada tecnología adoptada contribuya directamente al éxito empresarial.

Desde la Dirección Financiera y de quienes conforman el equipo de administración y finanzas, extendemos nuestras felicitaciones por este XIX aniversario a GrupoBeIT, del cual nos enorgullece ser parte.

Eduardo Navarro
GrupoBeIT
Director Financiero

Seguridad en aplicaciones web

Por: Elías Cedillo , Fundador y *CEO GrupoBeIT*

La seguridad de las aplicaciones web se ha convertido en una prioridad estratégica para las organizaciones. No se trata únicamente de proteger líneas de código, sino de salvaguardar la integridad de los datos, la confianza del cliente y la continuidad operativa.

La seguridad de las aplicaciones web abarca el conjunto de prácticas, herramientas y políticas destinadas a proteger sitios web, aplicaciones y APIs frente a amenazas externas. Su propósito es garantizar que estos sistemas funcionen correctamente y estén blindados contra ataques que puedan comprometer información sensible o interrumpir servicios.

La naturaleza abierta de Internet convierte a las aplicaciones en blancos accesibles desde cualquier parte del mundo. Esta exposición implica que los ataques pueden variar en escala, sofisticación y origen. Por ello, la protección de aplicaciones no puede limitarse a un solo punto: debe contemplar todo el ciclo de vida del software, desde el desarrollo hasta la operación.

Las empresas que manejan datos personales, financieros o estratégicos están especialmente en riesgo. Una brecha de seguridad puede traducirse en pérdidas económicas, sanciones legales y, lo más grave, la pérdida de confianza por parte de los usuarios. Implementar medidas de seguridad robustas no solo reduce la superficie de ataque, sino que también actúa como un escudo frente a prácticas desleales y ciberataques maliciosos.

Con la adopción masiva de servicios en la nube, los datos ya no residen en un solo lugar. Se distribuyen a través de múltiples redes y servidores, lo que puede complicar su protección. Aunque la seguridad de red sigue siendo esencial, proteger cada aplicación individual se ha vuelto igual de importante. Los atacantes ya no buscan solo vulnerabilidades en la infraestructura, sino que apuntan directamente a las aplicaciones como puerta de entrada.

Recomendar pruebas continuas, análisis de vulnerabilidades e implementación de soluciones preventivas permiten detectar fallos antes de que sean explotados. Este enfoque proactivo no solo reduce riesgos, sino que también fortalece la resiliencia de la organización frente a incidentes futuros.

Ignorar la seguridad de las aplicaciones puede tener consecuencias devastadoras: desde interrupciones operativas hasta daños irreparables en la reputación corporativa. Los usuarios esperan que sus datos estén protegidos, y cualquier fallo en este aspecto puede derivar en robo de identidad, fraudes o filtraciones masivas. La inversión en seguridad no es un gasto, sino una garantía de sostenibilidad y confianza.

Beneficios de la seguridad de las aplicaciones

- Disminución de interrupciones
- Detección temprana de problemas
- Mayor confianza del cliente
- Cumplimiento de requisitos normativos y de cumplimiento relacionados con la seguridad de los datos
- ·Mayor ahorro de costos
- Prevención de ciberataques, como malware y ransomware, inyecciones SQL y ataques de scripts entre sitios..
- Protección de datos sensibles
- Reducción de riesgos con la eliminación de vulnerabilidades aumenta la capacidad de prevenir ataques.
- Apoyo a la imagen de marca, al demostrar que la organización demuestra su compromiso en la protección de los datos de los clientes.

Una vez comprendida la importancia de proteger las aplicaciones web (redes sociales, plataformas de correos electrónicos, plataformas de streaming, plataformas de e-commers) es esencial conocer los tipos de ataques que pueden comprometer su seguridad. Las amenazas varían según los objetivos del atacante, el tipo de organización y las vulnerabilidades específicas de cada sistema. A continuación, se presentan los ataques más frecuentes que enfrentan las aplicaciones web en el entorno actual:

- Vulnerabilidades Zero-day: son fallos desconocidos por los desarrolladores que los atacantes explotan antes de que exista una solución. Cada año se detectan miles de estas vulnerabilidades, lo que representa un riesgo constante.
- Cross-site scripting (XSS): permite a los atacantes inyectar scripts maliciosos en páginas web para robar información, suplantar identidades o manipular la interacción del usuario.

- Inyección de código SQL (SQLi): mediante esta técnica, los atacantes acceden a bases de datos, alteran permisos o destruyen información confidencial.
- Ataques DoS y DDoS: saturan servidores con tráfico malicioso, provocando lentitud o interrupciones en el servicio, afectando a usuarios legítimos.
- Corrupción de memoria y desbordamiento de búfer: estas fallas técnicas permiten a los atacantes ejecutar código malicioso aprovechando errores en la gestión de la memoria del software.
- Falsificación de solicitud en sitios cruzados (CSRF): Engañan al usuario para que realice acciones no deseadas, aprovechando sus credenciales y privilegios.
- Relleno de credenciales: utilizando combinaciones robadas de usuario y contraseña, los atacantes acceden a cuentas reales para robar datos o realizar fraudes.
- Apropiación de páginas: Bots automatizados copian contenido web para fines maliciosos, como manipulación de precios o suplantación de identidad digital.
- Abuso de APIs: las interfaces de programación pueden ser vulnerables si no se protegen adecuadamente, permitiendo el robo o manipulación de datos entre aplicaciones.
- APIs paralelas: APIs no registradas por los equipos de seguridad pueden exponer información sensible sin que la organización lo sepa.
- Abuso de código de terceros: herramientas externas integradas en aplicaciones pueden ser un punto débil si no se auditan correctamente, como en los ataques Magecart.
- Desconfiguración de la superficie de ataque: elementos mal configurados o ignorados dentro de la infraestructura digital pueden dejar puertas abiertas a los atacantes.

Referencia:

Cloudflare

NOTICIA BeIT

Panorama Global

SHUYAL, el malware que rompe barreras y amenaza a 19 navegadores web.

Un nuevo y sofisticado malware ha irrumpido en el panorama de la ciberseguridad con una capacidad alarmante para robar credenciales: SHUYAL, un ladrón de información que no discrimina entre navegadores y que representa una amenaza sin precedentes para usuarios de todo tipo.

A diferencia de otros malwares que se enfocan en plataformas específicas, SHUYAL ha sido diseñado para atacar 19 navegadores web, desde los más populares como Google Chrome y Microsoft Edge, hasta opciones centradas en la privacidad como Tor y Epic Browser. Esta amplitud convierte a SHUYAL en una herramienta extremadamente peligrosa, capaz de comprometer a usuarios sin importar sus preferencias de navegación.

El ataque comienza con una fase de reconocimiento del sistema, seguida por la extracción de credenciales y la exfiltración de datos. SHUYAL no solo roba contraseñas: también captura pantallas del sistema, contenido del portapapeles y realiza un análisis detallado del entorno del usuario. Esta recopilación masiva de información permite a los atacantes construir perfiles completos de sus víctimas, facilitando fraudes más complejos e incluso el robo de identidad.

Uno de los aspectos más inquietantes de SHUYAL es su capacidad para evadir la detección. El malware desactiva automáticamente el Administrador de tareas de Windows, impidiendo que los usuarios puedan identificar procesos sospechosos. Además, modifica el registro del sistema para bloquear el acceso a herramientas de monitoreo, asegurando su permanencia en el dispositivo incluso después de reinicios.

SHUYAL utiliza canales de comunicación poco convencionales para enviar la información robada. Entre ellos se encuentran tokens de Discord y plataformas como Telegram, lo que le permite operar fuera del radar de muchas soluciones de seguridad tradicionales. Esta estrategia refuerza su capacidad de mantenerse oculto mientras realiza sus actividades maliciosas.

No es solo otro ladrón de contraseñas. Su diseño modular, su enfoque multiplataforma y sus técnicas avanzadas de evasión lo convierten en una amenaza de nueva generación. Representa un cambio en la forma en que los atacantes operan: ya no basta con proteger un navegador o una contraseña, ahora se requiere una estrategia integral de ciberseguridad que contemple todos los vectores posibles.

La aparición de SHUYAL es una llamada de atención urgente para usuarios, empresas y expertos en seguridad. La protección de credenciales ya no puede depender únicamente de buenas prácticas; se necesita tecnología avanzada, monitoreo constante y una cultura digital consciente del riesgo. En un mundo donde un solo malware puede vulnerar múltiples plataformas, la prevención es más crítica que nunca.

Referencia:
Cybersecuritynews

Sistema de Gestión de la Ciberseguridad Industrial (SGCI)

En el contexto actual de transformación digital y convergencia entre las tecnologías IT y OT, incluyendo la automatización y control industrial, enfrentan una creciente exposición a amenazas que comprometen su seguridad. Estas amenazas, tanto internas como externas, pueden manifestarse de múltiples formas: errores humanos, fallos técnicos, sabotajes, espionaje, vandalismo o incluso desastres naturales. La consecuencia directa es la aparición de incidentes que afectan la integridad, disponibilidad y confidencialidad de los activos informáticos de las organizaciones.

Aunque todos los sistemas de información comparten vulnerabilidades comunes, los entornos industriales presentan características particulares que amplifican los riesgos. La automatización de procesos productivos ha traído consigo mejoras significativas en eficiencia y productividad, gracias a la integración de tecnologías de la información y comunicaciones (TIC). Sin embargo, esta evolución también ha introducido nuevas debilidades y dependencias tecnológicas que, en muchos casos, no son gestionadas adecuadamente.

Uno de los principales retos en estos sistemas es la dificultad para realizar mantenimientos continuos. Las exigencias de disponibilidad en los procesos industriales limitan la posibilidad de aplicar actualizaciones o parches de seguridad, lo que genera un deterioro progresivo en la protección de los sistemas de control. Como resultado, muchas instalaciones operan con infraestructuras tecnológicas que no están preparadas para enfrentar las amenazas actuales.

Además, el creciente interés geopolítico en el ciberespacio como herramienta estratégica ha incrementado la exposición de los sistemas industriales a riesgos cibernéticos. La falta de mecanismos eficaces de gestión de ciberseguridad en muchas instalaciones industriales agrava esta situación, especialmente en procesos críticos para el negocio. A esto se suma la escasa cultura de ciberseguridad entre los profesionales involucrados en el ciclo de vida de estos sistemas, desde su diseño hasta su desmantelamiento.

Históricamente, la seguridad física ha recibido mayor atención que la ciberseguridad en entornos industriales. Esta disparidad ha dejado brechas importantes en la protección digital de infraestructuras clave. Además, la ausencia de normas específicas y modelos de gestión transversales dificulta la implementación de estrategias de seguridad adaptadas a las particularidades del sector industrial.

Ante esta realidad, se hace urgente el desarrollo de directrices específicas para la gestión de riesgos en sistemas de automatización y control industrial. Estas deben abordar de forma integral la protección de la información y operaciones, alineándose con los objetivos estratégicos de cada organización. Una propuesta efectiva es la creación de un Sistema de Gestión de la Ciberseguridad Industrial (SGCI), que contemple:

- Autonomía e integración: El SGCI debe ser independiente en su implementación, pero compatible con otros sistemas de gestión existentes, facilitando su adopción incluso en organizaciones con baja madurez en ciberseguridad.
- Agilidad operativa: Inicialmente, debe enfocarse en medidas básicas de protección, con posibilidad de expansión progresiva según las necesidades y capacidades de la empresa.

El Centro de Ciberseguridad Industrial (CCI) ha reconocido esta necesidad y ha desarrollado una guía para la construcción de un SGCI, estructurada en seis capítulos que abordan los dominios clave para su implementación. Esta iniciativa busca ofrecer un marco de referencia práctico y adaptable a distintos sectores industriales, promoviendo una gestión eficaz, eficiente y continua de la ciberseguridad brindando beneficios:

Contar con un SGCI alineado con los fundamentos del negocio no solo permite reducir los riesgos cibernéticos, sino que también aporta una serie de beneficios adicionales que respaldan su implementación dentro de la organización. Entre los más destacados se encuentran:

- Definición del riesgo tolerable: permite identificar el nivel de riesgo que la organización está dispuesta a asumir, lo cual es clave para establecer su perfil de riesgo.
- Alineación estratégica: facilita la integración del SGCI con la misión, visión y objetivos corporativos.
- Gestión de la cadena de suministro: considera los impactos relevantes en la cadena de suministro y promueve acciones para garantizar la continuidad operativa.
- Reducción de costos: minimiza los gastos asociados a incidentes de seguridad.
- Diligencia debida: demuestra el compromiso de la organización con la gestión responsable de la ciberseguridad, aspecto crucial ante posibles responsabilidades legales.
- Claridad organizativa: establece responsabilidades claras, identifica los componentes críticos del sistema y guía el desarrollo de políticas de ciberseguridad industrial.

- Mejora de la fiabilidad operativa: refuerza la disponibilidad y estabilidad de los sistemas más críticos.
- Condiciones laborales: contribuye a mejorar el entorno de trabajo y reduce la rotación de personal.
- Capacitación especializada: facilita la formación de profesionales en ciberseguridad industrial.
- Reputación corporativa: mejora la percepción pública y la confianza de terceros en la organización.
- Confianza de inversores: aumenta la credibilidad ante potenciales inversionistas.
- Reducción de responsabilidad civil: disminuye la exposición legal ante incidentes.
- Relación con aseguradoras: mejora las condiciones de contratación y cobertura.
- Cumplimiento normativo: ayuda a satisfacer requisitos legales, reglamentarios y contractuales.
- Resiliencia organizacional: refuerza la capacidad de la empresa para resistir y recuperarse ante eventos adversos.

Referencias:

Centro de Ciberseguridad Industrial - Guía para la construcción de un Sistema de Gestión de la Ciberseguridad Industrial (SGCI), 2016

BURÓMC SEGURIDAD INFORMÁTICA

ELIT INFRASTRUCTURE SERVICES

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

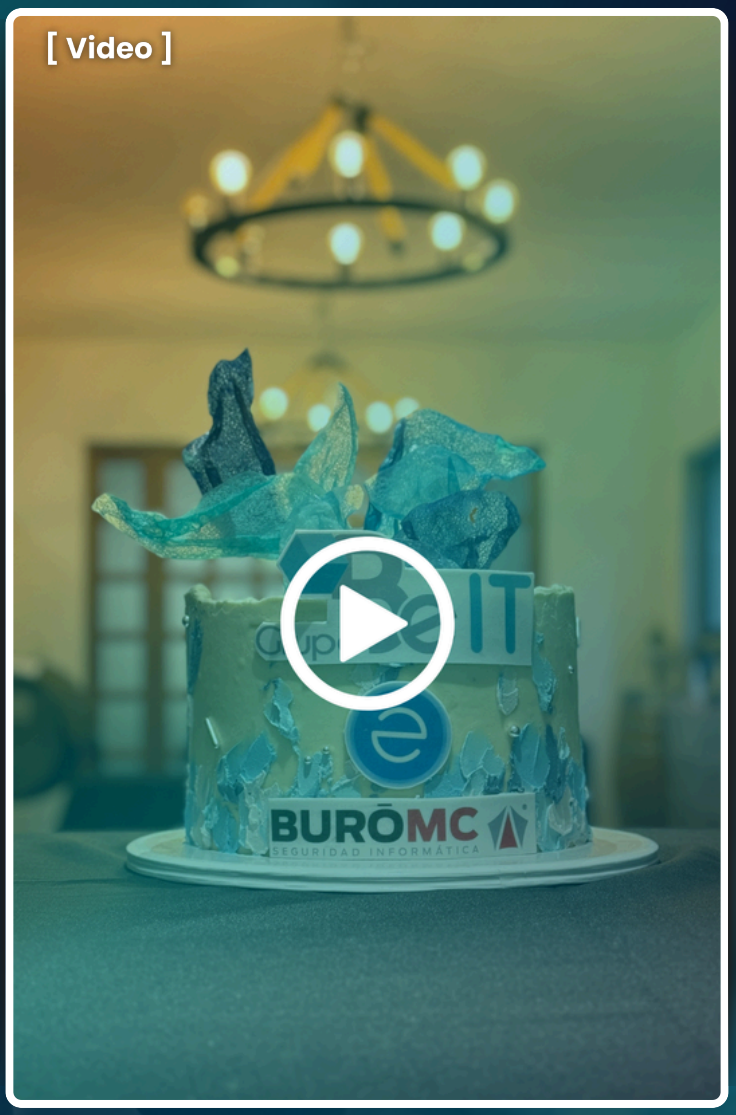
ó

Da clic o escanea el QR
y aparta tu lugar

Aniversario

SOCIAL BeIT

Da clic y disfruta lo que fue nuestra rueda de prensa conmemorativa



No te olvides de darle like y compartir.