Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Enero - 2026

Sobre Axus

Axus es una empresa especializada en ciberseguridad, con presencia en el Perú y Latinoamérica. Asesora a clientes en la protección de su información e infraestructura tanto en ámbitos industriales (OT) como en ámbitos corporativos (IT) y viene registrando una creciente participación en el ámbito de Internet de las Cosas (IoT) y en la protección de entornos Cloud e Híbridos.

En base a su reputación como especialista con los principales fabricantes de la industria y su equipo profesional en permanente capacitación, Axus genera valor a través de una visión consultiva que busca definir soluciones a la medida de las necesidades de cada cliente.

Alertas de Ciberseguridad

A continuación, compartimos con ustedes algunas de las alertas más relevantes de Enero.

Alertas de Seguridad IT:

- PcComponentes, empresa de comercio electrónico tecnológico, enfrenta intento de acceso no autorizado mediante ataque de credential stuffing
- MicroWorld Technologies (eScan), sufre compromiso de servidor de actualizaciones utilizado para distribuir malware
- Kyowon Group, conglomerado de servicios educativos y de consumo, confirma robo de datos tras ataque de ransomware

Alertas de Seguridad OT/ICS:

- Red Eléctrica de Polonia, sector energía, sufre ciberataque coordinado contra OT en aproximadamente 30 instalaciones DER
- Delta Electronics, fabricante de PLCs industriales, expone vulnerabilidades críticas en controladores usados en sectores sensibles asiáticos
- WestRock, empresa de empaques y manufactura, sufre ataque de ransomware que impacta sistemas OT e IT

PcComponentes, empresa de comercio electrónico tecnológico, enfrenta intento de acceso no autorizado mediante ataque de credential stuffing

Tipo de Ataque: Credential Stuffing

Medio de Propagación: Acceso web mediante credenciales filtradas en brechas previas

1. **PRODUCTOS AFECTADOS:**
   - Cuentas de clientes en la plataforma web de PcComponentes
2. **RESUMEN:**

PcComponentes detectó un incremento anómalo de intentos de inicio de sesión que llevó a la identificación de un ataque de credential stuffing. Un actor malicioso utilizó credenciales expuestas en incidentes de otras plataformas para intentar acceder a cuentas de usuarios dentro del portal de la compañía. Aunque se difundieron reclamos falsos sobre una supuesta filtración masiva de 16 millones de registros, la empresa confirmó que no hubo acceso ilegítimo a bases de datos internas ni sistemas corporativos. Durante la investigación se halló que los correos incluidos en muestras del atacante ya figuraban en registros de infostealers previos. Como parte de la contención, PcComponentes reforzó los mecanismos de autenticación y revisó los accesos potencialmente afectados.

3. **DETALLE:**

Un actor identificado como “daghetiaw” afirmó poseer 16.3 millones de registros de PcComponentes y publicó una muestra en foros clandestinos; sin embargo, la investigación interna no halló evidencia de intrusión ni exfiltración desde los sistemas de la compañía. El patrón observado corresponde a credential stuffing: uso automatizado de combinaciones de correo o contraseña previamente expuestas en otras brechas para validar accesos en el portal del minorista. La firma de inteligencia Hudson Rock indicó que los correos de la muestra del atacante coincidían con logs de infostealers existentes, algunos fechados desde 2020, lo que respalda que el vector fue la reutilización de credenciales y no una vulnerabilidad propia del entorno de PcComponentes. Como respuesta, la empresa habilitó CAPTCHA, invalidó sesiones activas y exigió 2FA para todos los usuarios; además, señaló que no almacena datos financieros, por lo que no se comprometieron detalles bancarios. Este comportamiento puede derivar en acceso a datos de perfil, modificación de direcciones o intentos de compra fraudulenta a nivel de cuenta, sin implicar un acceso a la base de datos central.

4. **RECOMENDACIONES:**
   - Implementar segmentación estricta entre redes IT y OT, con firewalls y listas de control de acceso granulares.
   - Actualizar y parchear sistemas y aplicaciones críticas; endurecer configuraciones (CIS benchmarks) en servidores y endpoints.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/online-retailer-pccomponentes-says-data-breach-claims-are-fake/

MicroWorld Technologies (eScan), sufre compromiso de servidor de actualizaciones utilizado para distribuir malware

Tipo de Ataque: **Compromiso de cadena de suministro / Distribución de actualización maliciosa**

Medio de Propagación: **Actualización de software a través de infraestructura legítima de eScan**

1. **PRODUCTOS AFECTADOS:**
   - Clientes corporativos y de consumo que descargaron actualizaciones desde el clúster regional
   - Componente modificado Reload.exe (parte del mecanismo de actualización)
2. **RESUMEN:**

Un servidor regional de actualizaciones de eScan fue comprometido, permitiendo que los atacantes insertaran un archivo malicioso dentro del flujo legítimo de actualizaciones. Durante una ventana aproximada de dos horas, usuarios que descargaron actualizaciones desde dicho clúster recibieron un paquete alterado que distribuía software malicioso. El incidente fue detectado inicialmente por reportes internos y posteriormente confirmado por análisis externos. eScan aisló y reconstruyó la infraestructura afectada, además de notificar a los clientes impactados.

3. **DETALLE:**

El ataque se originó mediante acceso no autorizado a la configuración de un servidor de actualizaciones de eScan, permitiendo a los atacantes sustituir un archivo legítimo por un componente malicioso dentro de la ruta de distribución. El archivo comprometido, una versión modificada de Reload.exe, aparentaba estar firmado con un certificado de eScan, aunque con una firma inválida, facilitando su ejecución en los endpoints afectados. Una vez ejecutado, el componente establecía persistencia mediante tareas programadas que simulaban procesos del sistema (ej. “CorelDefrag”) y modificaba el archivo HOSTS para bloquear la comunicación con los servidores de eScan. Posteriormente, descargaba payloads adicionales desde infraestructura C2, siendo CONSCTLX.exe el backdoor final desplegado, capaz de ejecutar comandos, alterar configuraciones del sistema y mantener comunicación continua con los servidores de los atacantes. El malware incorporaba mecanismos anti-remediación que impedían la actualización automática del antivirus, prolongando la permanencia de la infección. Este vector representa un ataque de cadena de suministro altamente dirigido, utilizando canales legítimos para comprometer endpoints sin necesidad de intervención del usuario.

4. **RECOMENDACIONES:**
   - Implementar revisión inmediata de endpoints en busca de los archivos maliciosos Reload.exe y CONSCTLX.exe.
   - Restaurar configuraciones del archivo HOSTS y claves de registro relacionadas con eScan.
   - Fortalecer el control de integridad y autenticación en servidores de actualización internos.
5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/escan-confirms-update-server-breached-to-push-malicious-update/

Kyowon Group, conglomerado de servicios educativos y de consumo, confirma robo de datos tras ataque de ransomware

Tipo de Ataque: Ransomware con exfiltración de datos

Medio de Propagación: Intrusión en servidores corporativos y movimiento lateral dentro de la red interna

1. **PRODUCTOS AFECTADOS:**
   - Servidores corporativos de Kyowon Group (aprox. 600 de 800 afectados)
   - Bases de datos internas con 9.6 millones de cuentas potencialmente comprometidas
2. **RESUMEN:**

Kyowon Group confirmó que sufrió un ataque de ransomware que interrumpió sus operaciones y resultó en la exfiltración no autorizada de datos. El incidente fue detectado tras interrupciones en diversos servicios y análisis de actividad anómala en sus sistemas internos. Según las primeras investigaciones, aproximadamente 600 servidores fueron comprometidos y existe la posibilidad de exposición de información perteneciente a millones de usuarios. La compañía ha aislado la infraestructura afectada, activado protocolos de emergencia y está colaborando con las autoridades coreanas (KISA) para determinar el alcance real de la filtración.

3. **DETALLE**

La intrusión comenzó con el acceso indebido a un servidor expuesto, el cual fue utilizado para infiltrarse en la red interna de Kyowon, desencadenando un despliegue de ransomware que se propagó lateralmente entre múltiples subsidiarias. El atacante aprovechó un puerto externo abierto que permitió el ingreso al entorno corporativo, afectando servicios críticos y bases de datos internas. Posteriormente, el ransomware bloqueó sistemas y provocó la desconexión forzosa de varias plataformas, lo que llevó a la interrupción de servicios educativos, de consumo y soporte al cliente. Investigaciones preliminares confirman indicios de robo de información, aunque todavía no se ha determinado si los datos personales de usuarios fueron incluidos. La compañía está ejecutando acciones para estabilizar sus sistemas, restaurar servicios y coordinar con expertos externos para verificar el alcance del daño, evaluar la exfiltración y contener la actividad maliciosa residual.

4. **RECOMENDACIONES:**
   - Implementar un análisis forense completo en los sistemas afectados para identificar vectores de acceso y actividad maliciosa.
   - Actualizar y reforzar controles de acceso a servicios expuestos a Internet, eliminando puertos abiertos no esenciales.
   - Fortalecer los mecanismos de monitoreo, detección temprana y respuesta ante intrusiones en la red corporativa.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/south-korean-giant-kyowon-confirms-data-theft-in-ransomware-attack/

Red Eléctrica de Polonia, sector energía, sufre ciberataque coordinado contra OT en aproximadamente 30 instalaciones DER

Tipo de Ataque: Intrusión y sabotaje en OT/ICS con wiping y corrupción de configuraciones

Medio de Propagación: Sistemas en el borde de red/telecontrol y equipos Windows en sitios DER

1. **PRODUCTOS AFECTADOS:**
   - RTUs y dispositivos de comunicaciones grid-facing en sitios DER (CHP, eólico y solar).
   - Sistemas de monitoreo y control (SCADA locales/telecontrol) con pérdida de visibilidad y mando remoto.
   - Hosts Windows en plantas afectadas (wiping y corrupción de configuraciones)
2. **RESUMEN:**

Un ataque coordinado impactó múltiples recursos energéticos distribuidos (DER) en Polonia, plantas de cogeneración (CHP) y sistemas de despacho eólico/solar, logrando acceso a sistemas OT, inutilizando equipos clave y provocando pérdida de monitoreo y control en varios emplazamientos. Pese al daño, no se produjeron apagones, y la generación continuó operando; el alcance estimado ronda 30 sitios (al menos 12 confirmados públicamente). El incidente subraya la vulnerabilidad del modelo descentralizado y el potencial de desestabilizar la frecuencia aun sin corte masivo.

3. **DETALLE:**

El adversario dirigió sus acciones a la frontera OT de la red: RTUs, dispositivos en el borde de red y enlaces de despacho que enlazan DER con el operador, además de equipos Windows en sitio. La táctica consistió en comprometer configuraciones comunes entre múltiples instalaciones, demostrando conocimiento profundo de despliegues y operación, y repitiendo los mismos patrones de intrusión para escalar el impacto. En varios puntos, el atacante deshabilitó comunicaciones, generando pérdida de vista y control, mientras que ciertos dispositivos OT/ICS quedaron inutilizados y configuraciones fueron corrompidas sin posibilidad de recuperación; los sistemas Windows fueron borrados. Aunque no hubo desconexión de carga, los analistas advierten que, de haberse ejecutado comandos operacionales coordinados, podrían haberse provocado desviaciones de frecuencia con fallos en cascada. Dragos atribuye con confianza moderada a Electrum, históricamente asociado a malware OT como Industroyer2 y wipers (Caddywiper, DynoWiper), y señala que el operativo representa el primer ataque mayor enfocado en DER a escala.

4. **RECOMENDACIONES:**
   - Segmentar estrictamente redes OT/IT y aislar RTUs/telecontrol del acceso directo a Internet; desplegar firewalls industriales y DMZ para despacho DER.
   - Endurecer el borde OT: inventariar y deshabilitar servicios expuestos, aplicar gestión de parches/configuración y listas de control por protocolo industrial.
   - Planificar respuesta en DER (procedimientos de recuperación para equipos “bricked”).

5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/cyberattack-on-polish-energy-grid-impacted-around-30-facilities/

Delta Electronics, fabricante de PLCs industriales, expone vulnerabilidades críticas en controladores usados en sectores sensibles asiáticos

Tipo de Ataque: Vulnerabilidades críticas en PLC (riesgo de explotación remota)

Medio de Propagación: Paquetes enviados al PLC sin autenticación, explotación remota de fallas en firmware

1. **PRODUCTOS AFECTADOS:**
   - PLC Delta Electronics DVP-12SE11T
   - Funcionalidades internas de autenticación y gestión de memoria del firmware
   - Sectores afectados: agua, alimentos y bebidas, manufactura, automatización y robótica
2. **RESUMEN:**

Investigadores de OPSWAT Unit 515 identificaron cuatro vulnerabilidades de alta y crítica severidad en el PLC Delta DVP-12SE11T, ampliamente utilizado en instalaciones industriales de Asia. Tres de los fallos alcanzan puntajes superiores a 9.0 CVSS, comprometiendo funciones esenciales del controlador. Estas vulnerabilidades permiten bypass de autenticación, filtración de información de contraseñas, congelamiento del dispositivo y escritura fuera de límites. Expertos advierten que estas fallas podrían permitir manipulación directa de procesos físicos, afectando seguridad, producción y continuidad operacional.

3. **DETALLE:**

Los investigadores, APT41 o UNC3886, podrían explotar este tipo de PLCs por su presencia en sectores sensibles. Aunque el firmware corregido ya está disponible, muchos entornos OT no aplicarán el parche de inmediato debido a limitaciones operativas y alta criticidad de sus procesos. Además, se advierte que incluso sin explotar estas vulnerabilidades, muchos PLC operan con comunicaciones no autenticadas que permiten modificar procesos directamente si se alcanza la red OT, incrementando aún más el riesgo operacional.

4. **RECOMENDACIONES:**
   - Implementar segmentación estricta entre redes IT y OT.
   - Aplicar políticas de contraseñas robustas y habilitar autenticación multifactor en todo acceso a sistemas SCADA.
   - Actualizar firmware, software y parches de controladores, servidores SCADA y endpoints asociados.
   - Deshabilitar servicios expuestos innecesarios y asegurar RDP/VPN con configuraciones endurecidas.
5. **REFERENCIAS:**

- https://www.darkreading.com/ics-ot-security/critical-bugs-delta-industrial-plcs

WestRock, empresa de empaques y manufactura, sufre ataque de ransomware que impacta sistemas OT e IT

Tipo de Ataque: Ransomware

Medio de Propagación: Intrusión en red corporativa con afectación tanto en sistemas IT como OT

1. **PRODUCTOS AFECTADOS:**
   - Sistemas IT corporativos de WestRock destinados a soporte operativo.
   - Sistemas OT utilizados en plantas de producción, conversión y operaciones industriales.
   - Infraestructura de control y monitoreo en operaciones de manufactura.
2. **RESUMEN:**

WestRock, uno de los mayores fabricantes de empaques, confirmó haber sido víctima de un ataque de ransomware descubierto el 23 de enero, el cual comprometió simultáneamente sus sistemas IT y OT. Como resultado, la empresa experimentó retrasos en operaciones, afectaciones en la producción y posibles impactos financieros. Tras detectar el incidente, WestRock activó protocolos de respuesta, aisló sistemas y notificó a las autoridades pertinentes, mientras trabajaba para restaurar su infraestructura y mantener la continuidad del negocio.

3. **DETALLE:**

El ataque consistió en la infiltración de un ransomware que logró impactar tanto la capa IT como la capa OT de la organización. La afectación a OT provocó la ralentización de operaciones críticas en mills y plantas de conversión, reduciendo significativamente la capacidad productiva planificada. WestRock inició esfuerzos acelerados de contención, apoyándose en firmas de ciberdefensa, e implementó procesos manuales para mitigar la interrupción operativa mientras los sistemas afectados eran restaurados. Aunque no se divulgaron detalles técnicos del vector inicial, se sabe que la infección provocó la desconexión preventiva de varios sistemas y la activación de procedimientos de continuidad. Las consecuencias operativas incluyeron retrasos en envíos, disminución de capacidad productiva y potencial impacto financiero por costos incrementales asociados al ataque. Paralelamente, la empresa continúa evaluando el alcance real sobre sistemas industriales, destacando la vulnerabilidad inherente de entornos OT frente a este tipo de amenazas.

4. **RECOMENDACIONES:**
   - Aislar equipos industriales vulnerables y segmentar adecuadamente las redes OT para mitigar propagación futura.
   - Actualizar políticas de monitoreo en entornos OT, incorporando detección activa de comportamientos anómalos.
   - Fortalecer controles de acceso y mecanismos de autenticación en dispositivos OT.

5. **REFERENCIAS:**

- https://www.securityweek.com/packaging-giant-westrock-says-ransomware-attack-impacted-ot-systems/