Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Agosto - 2025

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 Agosto.

Alertas de Seguridad IT:

- TransUnion sufre brecha de datos que afecta a más de 44 millones de personas
- Wytec, empresa estadounidense de telecomunicaciones, sufre hackeo y caída de su sitio web
- Miljödata, proveedor sueco de TI, provoca interrupción masiva en 200 municipios por ataque de ransomware

Alertas de Seguridad OT/ICS:

- Inotiv, empresa farmacéutica estadounidense, interrumpe operaciones tras ataque de ransomware atribuido a Qilin
- Data I/O Corporation, fabricante de sistemas electrónicos, sufre ataque de ransomware que paraliza operaciones críticas
- Jaguar Land Rover, fabricante de automóviles, paraliza producción global tras ciberataque con robo de datos

TransUnion sufre brecha de datos que afecta a más de 44 millones de personas

Tipo de Ataque: **Exposición de Información / Brecha de Datos**

Medio de Propagación: **Acceso no autorizado a sistemas internos**

1. **PRODUCTOS AFECTADOS:**
   - Bases de datos de clientes
   - Sistemas de gestión de identidad
   - Plataformas de análisis crediticio
   - Infraestructura de TI corporativa

2. **RESUMEN:**

TransUnion, una de las principales agencias de informes crediticios, confirmó una brecha de seguridad que expuso información personal de más de 44 millones de personas. El incidente fue detectado tras una investigación interna y se atribuye a accesos no autorizados a sus sistemas. Los datos comprometidos incluyen nombres, direcciones, números de identificación y detalles financieros.

3. **DETALLE:**

El ataque se originó por una intrusión en los sistemas de TI de TransUnion, donde actores maliciosos lograron acceder a bases de datos sensibles. Aunque no se ha confirmado el vector exacto, este tipo de brechas suelen estar relacionadas con vulnerabilidades en aplicaciones web, credenciales comprometidas o configuraciones incorrectas en servicios expuestos a internet. El atacante pudo extraer grandes volúmenes de información sin ser detectado inicialmente, lo que sugiere una falta de monitoreo efectivo y controles de acceso robustos.

4. **RECOMENDACIONES:**
   - Reforzar controles de acceso y autenticación multifactor
   - Auditar configuraciones de seguridad en bases de datos y servidores
   - Implementar monitoreo continuo de accesos y actividades sospechosas
   - Actualizar sistemas y aplicaciones con los últimos parches de seguridad
   - Cifrar datos sensibles tanto en tránsito como en reposo
   - Notificar a los usuarios afectados y ofrecer servicios de protección de identidad
   - Establecer políticas de respuesta ante brechas de datos

5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/transunion-suffers-data-breach-impacting-over-44-million-people/

Wytec, empresa estadounidense de telecomunicaciones, sufre hackeo y caída de su sitio web

Tipo de Ataque: **Defacement Web (con posible exfiltración de datos)**

Medio de Propagación: **Navegador / Plataforma Web**

1. **PRODUCTOS AFECTADOS:**
   - Sitio web corporativo (wytecintl.com)
   - Plataforma de gestión de eventos y seminarios
   - Infraestructura web pública y backend asociado

2. **RESUMEN:**

El 25 de agosto de 2025, Wytec International, proveedor de soluciones de telecomunicaciones y seguridad con sede en Texas, fue víctima de un ciberataque que resultó en la defacement de su sitio web. Aunque la empresa restauró el sitio desde respaldos, los atacantes lograron vulnerarlo nuevamente. El sitio permanece fuera de línea mientras se realiza una revisión completa de la plataforma. La empresa notificó al FBI y contrató especialistas forenses. Como consecuencia, se canceló un seminario programado para el 2 de septiembre, generando pérdidas financieras significativas.

3. **DETALLE**

El ataque consistió en la alteración visual del sitio web (defacement), lo que indica acceso no autorizado al servidor web. La persistencia del atacante, que logró vulnerar el sitio dos veces, sugiere fallas en la seguridad de la plataforma, posiblemente por credenciales comprometidas o falta de segmentación adecuada. Según reportes financieros, se estima que **hasta 6.4 millones de registros** podrían haber sido comprometidos, incluyendo datos personales y bancarios, aunque esto aún está bajo investigación.

Wytec informó una caída del 26.92% en el valor de sus acciones tras el incidente, y enfrenta riesgos reputacionales y regulatorios. La empresa está implementando medidas de seguridad adicionales y mantiene el sitio en modo de mantenimiento mientras se valida la integridad de la infraestructura.

4. **RECOMENDACIONES:**
   - Implementar autenticación multifactor en accesos administrativos
   - Realizar auditoría de seguridad en servidores web y CMS
   - Activar monitoreo continuo de integridad de archivos y logs
   - Restringir accesos externos a paneles de administración
   - Establecer políticas de restauración segura desde respaldos y capacitar al equipo técnico en respuesta ante incidentes web
   - Notificar a usuarios si se confirma exfiltración de datos

5. **REFERENCIAS:**

- https://www.securityweek.com/wytec-expects-significant-financial-loss-following-website-hack/

Miljödata, proveedor sueco de TI, provoca interrupción masiva en 200 municipios por ataque de ransomware

Tipo de Ataque: Ransomware (doble extorsión)
Medio de Propagación: Red Interna / Plataforma de gestión administrativa

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de gestión de recursos humanos (Adato, Stella, Novi)
   - Infraestructura de TI de más de 200 municipios y regiones suecas
2. **RESUMEN:**

El 23 de agosto de 2025, el proveedor sueco de servicios TI **Miljödata** sufrió un ataque de ransomware que afectó a más de **200 municipios** y regiones del país. La empresa, que presta servicios a aproximadamente el 80% de las administraciones locales, vio comprometidos sus sistemas de gestión de RRHH, certificados médicos y reportes de lesiones laborales. El ataque provocó la caída de servicios esenciales, y se estima que datos personales sensibles podrían haber sido expuestos. Las autoridades suecas, incluyendo **CERT-SE** y la **Agencia de Protección de Datos (IMY)**, están investigando el incidente.

3. **DETALLE:**

El ataque fue identificado como un caso de **ransomware de doble extorsión**, donde los sistemas fueron cifrados y se exigió un rescate de **1.5 Bitcoin (aproximadamente $168,000)** para evitar la filtración de datos robados. Aunque no se ha confirmado públicamente qué grupo está detrás del ataque, se sabe que los sistemas afectados incluían plataformas críticas como **Adato** (gestión de licencias médicas), **Stella** (reportes de lesiones laborales) y **Novi** (gestión de RRHH).

El proveedor **Miljödata** aisló sus sistemas para contener el ataque, lo que dejó fuera de servicio múltiples plataformas utilizadas por municipios como Gotland, Halland, Kalmar, Karlstad, Skellefteå y otros. Las autoridades locales han advertido que **información médica, planes de rehabilitación y datos laborales** podrían haber sido comprometidos. El gobierno sueco está evaluando el impacto y ha anunciado una futura ley de ciberseguridad para fortalecer la protección de infraestructuras críticas.

4. **RECOMENDACIONES:**
   - Auditar la seguridad de proveedores externos que gestionan datos sensibles
   - Implementar segmentación de redes y controles de acceso en plataformas compartidas
   - Establecer protocolos de respuesta ante incidentes con proveedores críticos
   - Evaluar el cumplimiento de normativas como GDPR y reportar incidentes en los plazos establecidos
   - Fortalecer la resiliencia de la cadena de suministro digital mediante acuerdos contractuales de ciberseguridad
5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/it-system-supplier-cyberattack-impacts-200-municipalities-in-sweden/

Inotiv, empresa farmacéutica estadounidense, interrumpe operaciones tras ataque de ransomware atribuido a Qilin

Tipo de Ataque: Ransomware con Exfiltración de Datos

Medio de Propagación: Red Interna / Sistemas de almacenamiento y aplicaciones empresariales

1. PRODUCTOS AFECTADOS:

- Sistemas de almacenamiento interno de datos
- Aplicaciones empresariales para investigación y desarrollo farmacéutico
- Infraestructura de TI en centros de investigación de Inotiv

2. RESUMEN:

El 8 de agosto de 2025, Inotiv, empresa estadounidense especializada en investigación y desarrollo de medicamentos, detectó un ciberataque que afectó sus sistemas internos. El incidente obligó a la compañía a cerrar temporalmente partes de su infraestructura tecnológica, lo que provocó interrupciones operativas en sus procesos de investigación. El grupo de ransomware Qilin se atribuyó el ataque, afirmando haber robado 176 GB de datos que incluyen 162,000 archivos recopilados durante los últimos 10 años. La empresa notificó a las autoridades y continúa trabajando en la restauración de sus sistemas.

3. DETALLE:

El ataque fue ejecutado por el grupo **Qilin**, una organización de ransomware-as-a-service (RaaS) que ofrece malware personalizado en lenguajes como Rust y Go, dirigido a entornos Windows, Linux y VMware ESXi. El grupo accedió de forma no autorizada a los sistemas de Inotiv, cifrando archivos y aplicaciones críticas utilizadas en la investigación de medicamentos, evaluación de seguridad y modelado con animales vivos.

La empresa activó su estrategia de continuidad de negocio, migrando operaciones afectadas a sistemas offline para mitigar el impacto. Sin embargo, la disponibilidad de redes internas, almacenamiento de datos y aplicaciones empresariales se vio comprometida, generando una interrupción significativa en las operaciones. Aunque Inotiv no ha confirmado si se realizó un pago de rescate, el grupo Qilin publicó muestras de los datos robados en su sitio de filtraciones en la dark web. La investigación forense sigue en curso, y aún no se ha determinado el impacto financiero total ni la extensión completa de la brecha.

4. RECOMENDACIONES:

- Establecer un marco de ciberresiliencia para entornos de investigación y OT, que contemple continuidad operativa, segmentación de red y recuperación ante desastres.
- Integrar inteligencia de amenazas en tiempo real, con correlación de indicadores de compromiso y automatización de respuestas para detectar y contener intrusiones antes de que escalen.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/pharma-firm-inotiv-says-ransomware-attack-impacted-operations/

Data I/O Corporation, fabricante de sistemas electrónicos, sufre ataque de ransomware que paraliza operaciones críticas

Tipo de Ataque: Ransomware

Medio de Propagación: Red Interna

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de manufactura
   - Plataforma de producción
   - Servicios de embarque y soporte
   - Infraestructura de TI global
2. **RESUMEN:**

El 16 de agosto de 2025, Data I/O Corporation, empresa con sede en Redmond especializada en componentes electrónicos para vehículos y dispositivos de consumo, reportó un ataque de ransomware ante la SEC. El incidente provocó la interrupción de sistemas críticos relacionados con manufactura, embarque y soporte. La empresa activó medidas de contención y está a la espera de una investigación externa para determinar el alcance del compromiso.

3. **DETALLE:**

El ataque se originó en la red interna de la empresa, donde actores maliciosos lograron desplegar ransomware que cifró sistemas operativos esenciales. La propagación afectó funciones clave como producción y logística, lo que obligó a desconectar sistemas para evitar una mayor afectación. Aunque no se ha confirmado el vector inicial, se presume que el acceso pudo haberse logrado mediante credenciales comprometidas o vulnerabilidades en servicios expuestos. La falta de segmentación y controles de acceso contribuyó a la expansión del malware. La empresa indicó que los costos derivados del incidente, incluyendo asesoría especializada y restauración de sistemas, tendrán un impacto material en sus resultados financieros. Aún no se ha determinado si hubo exfiltración de datos ni se ha establecido una fecha para la restauración total de servicios.

4. **RECOMENDACIONES:**
   - Implementar segmentación de red para limitar la propagación de amenazas
   - Activar autenticación multifactor en accesos administrativos y remotos
   - Restringir privilegios innecesarios en cuentas de usuario
   - Realizar copias de seguridad periódicas y almacenarlas fuera de línea
   - Actualizar sistemas con los últimos parches de seguridad
   - Monitorear continuamente la red en busca de comportamientos anómalos
   - Establecer protocolos de respuesta ante incidentes y simulacros regulares

5. **REFERENCIAS:**

- https://therecord.media/electronics-manufacturer-dataio-ransomware

Jaguar Land Rover, fabricante de automóviles, paraliza producción global tras ciberataque con robo de datos

Tipo de Ataque: Ransomware con Exfiltración de Datos

Medio de Propagación: Red Interna / Aplicaciones empresariales (SAP, Jira)

1. PRODUCTOS AFECTADOS:

- Sistemas de producción en plantas de Reino Unido, India, China, Eslovaquia y Brasil
- Aplicaciones empresariales (SAP, Jira, sistemas de registro de vehículos)
- Infraestructura de ventas, logística y distribución global
- Sistemas de atención al cliente y concesionarios

2. RESUMEN:

A fines de agosto de 2025, Jaguar Land Rover (JLR), subsidiaria de Tata Motors, sufrió un ciberataque que obligó a suspender la producción en todas sus plantas globales. El incidente afectó sistemas críticos de manufactura, ventas y logística, dejando a más de 33,000 empleados sin actividad. La empresa confirmó el robo de datos sensibles y notificó a los reguladores. El grupo "Scattered Lapsus$ Hunters", vinculado a Lapsus$, Scattered Spider y ShinyHunters, se atribuyó el ataque, compartiendo capturas de sistemas internos. La recuperación ha sido lenta y costosa, con pérdidas estimadas en más de £50 millones semanales.

3. DETALLE:

El ataque fue ejecutado por un colectivo de cibercriminales que accedió a sistemas internos de JLR, incluyendo SAP y Jira, mediante técnicas de ingeniería social, uso de credenciales robadas y explotación de tokens OAuth. Se detectó exfiltración de datos técnicos, credenciales de empleados, y documentos internos. El grupo publicó evidencia en Telegram, incluyendo archivos de configuración y pantallas de sistemas internos. La interrupción afectó la producción de más de 1,000 vehículos diarios, paralizó el registro de autos nuevos y la entrega de repuestos. El gobierno británico otorgó un préstamo garantizado de £1.5 mil millones para mitigar el impacto en la cadena de suministro. La empresa continúa trabajando con el NCSC y especialistas forenses para restaurar sus sistemas de forma segura.

4. RECOMENDACIONES:

- Implementar segmentación estricta entre redes IT y OT
- Activar monitoreo de comportamiento y detección de anomalías en sistemas críticos y aplicar autenticación multifactor
- Auditar y reforzar la seguridad de aplicaciones empresariales (SAP, Jira)
- Establecer protocolos de respuesta ante incidentes con simulacros regulares

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/jaguar-land-rover-extends-shutdown-after-cyberattack-by-another-week/