Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Mayo - 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 Abril.

Alertas de Seguridad IT:

- Krispy Kreme sufre ciberataque que afecta pedidos en línea y operaciones comerciales
- Gobierno del Perú sufre presunto ciberataque con demanda de rescate millonaria
- MathWorks confirma ciberataque con ransomware como causa de interrupciones en sus servicios

Alertas de Seguridad OT/ICS:

- Arla Foods confirma ciberataque que interrumpe su producción y causa retrasos
- China vinculada a ciberataques contra el sector de drones mediante compromisos en la cadena de suministro
- Masimo confirma ciberataque que afecta sus instalaciones de manufactura

Krispy Kreme sufre ciberataque que afecta pedidos en línea y operaciones comerciales

Tipo de Ataque: Ciberataque a infraestructura IT

Medio de Propagación: Acceso no autorizado a sistemas internos

1. **PRODUCTOS AFECTADOS:**
   - Plataforma de pedidos en línea de **Krispy Kreme**

2. **RESUMEN:**

Krispy Kreme, la reconocida cadena estadounidense de donas, confirmó que fue víctima de un ciberataque que interrumpió su capacidad para procesar pedidos en línea y afectó partes de sus operaciones internas. El incidente, detectado en mayo de 2025, obligó a la empresa a tomar medidas de contención mientras trabaja en la restauración de sus servicios.

3. **DETALLE:**

El ataque afectó la infraestructura IT de Krispy Kreme, provocando la caída de su sistema de pedidos en línea y generando retrasos en la atención al cliente. Aunque la empresa no ha revelado si se trató de un ataque de ransomware o de otro tipo, sí confirmó que está trabajando con expertos en ciberseguridad para investigar el incidente y mitigar sus efectos.

Krispy Kreme no ha informado sobre filtración de datos de clientes hasta el momento, pero ha recomendado a los usuarios estar atentos a comunicaciones oficiales y posibles intentos de fraude. La empresa continúa restaurando gradualmente sus servicios digitales.

Este incidente refleja la creciente exposición de las cadenas minoristas a amenazas cibernéticas que pueden afectar tanto la experiencia del cliente como la continuidad operativa.

4. **RECOMENDACIONES:**
   - Supervisar cuentas asociadas a pedidos recientes y estar alerta ante correos sospechosos.
   - Cambiar contraseñas si se utilizó la misma en otros servicios.
   - Las empresas deben implementar monitoreo continuo, segmentación de redes y planes de recuperación ante incidentes.
   - Realizar auditorías de seguridad periódicas y pruebas de penetración.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/krispy-kreme-cyberattack-impacts-online-orders-and-operations/

Gobierno del Perú sufre presunto ciberataque con demanda de rescate millonaria

Tipo de Ataque: Ransomware

Medio de Propagación: Intrusión en sistemas web mediante malware del tipo Rhysida

1. **PRODUCTOS AFECTADOS:**
   - Sitio web oficial del Gobierno del Perú (**gob.pe**)

2. **RESUMEN:**

El 2 de mayo de 2025, el portal oficial del Gobierno del Perú fue blanco de un ciberataque atribuido al grupo de ransomware **Rhysida**, el cual exigió un rescate de **54 bitcoins** (equivalente a aproximadamente **S/ 1.77 millones**) para no divulgar información sensible. Aunque el sitio web fue restablecido tras una breve interrupción, el incidente generó preocupación sobre la seguridad de la infraestructura digital del Estado

3. **DETALLE**

Según reportes de la plataforma DarkWeb Informer, los atacantes afirmaron haber accedido a documentos oficiales y amenazaron con publicarlos si no se cumplía con el pago en un plazo de siete días. El grupo Rhysida es conocido por utilizar tácticas de ransomware para extorsionar a entidades públicas y privadas.

Sin embargo, el Gobierno peruano, a través de la Secretaría de Gobierno y Transformación Digital de la PCM, negó que la plataforma **www.gob.pe** haya sido vulnerada. Afirmaron que el sitio ha funcionado con normalidad y que los datos están respaldados y seguros. También aclararon que el dominio afectado podría haber sido **gob.pe**, que pertenece a la Red Científica Peruana, y no el portal oficial del Estado.

A pesar de la negación oficial, las capturas divulgadas por los atacantes y la caída temporal del sitio han generado dudas sobre la magnitud real del incidente y la posible exposición de información gubernamental.

4. **RECOMENDACIONES:**
   - Priorizar controles de acceso sólidos y actualizaciones periódicas del sistema para mitigar el riesgo de ataques de ransomware.
   - de ciberseguridad efectivas.

5. **REFERENCIAS:**
   - https://www.infobae.com/peru/2025/05/02/gobierno-de-peru-es-victima-de-ataque-cibernetico-hackers-piden-s-17-millones-para-recuperar-web-del-estado/

MathWorks confirma ciberataque con ransomware como causa de interrupciones en sus servicios

Tipo de Ataque: Ransomware
Medio de Propagación: Intrusión en sistemas internos seguida de cifrado de datos

1. **PRODUCTOS AFECTADOS:**
   - Servicios en línea de **MathWorks** (MATLAB Central, Portales de licencias y soporte)
2. **RESUMEN:**

MathWorks, desarrollador de MATLAB y Simulink, confirmó que un ataque de ransomware es responsable de las interrupciones en sus servicios que comenzaron a finales de mayo de 2025. La empresa informó que el incidente afectó su infraestructura interna, lo que ha provocado dificultades para acceder a servicios clave utilizados por ingenieros, investigadores y desarrolladores en todo el mundo.

3. **DETALLE:**

El ataque fue revelado públicamente el 27 de mayo de 2025, cuando MathWorks reconoció que sus sistemas habían sido comprometidos por actores maliciosos que desplegaron ransomware. Aunque la compañía no ha especificado el grupo responsable ni el método exacto de intrusión, se sabe que el ataque afectó la disponibilidad de servicios esenciales como la activación de licencias, descargas de software y acceso a recursos comunitarios.

MathWorks aseguró que está trabajando con expertos en ciberseguridad y autoridades para contener el incidente, restaurar los servicios y proteger los datos de los usuarios. Hasta el momento, no se ha confirmado si hubo filtración de información confidencial.

Este incidente subraya la creciente amenaza del ransomware contra empresas tecnológicas y académicas, especialmente aquellas que ofrecen servicios críticos en línea.

4. **RECOMENDACIONES:**
   - Realizar copias de seguridad frecuentes y almacenarlas fuera de línea.
   - Implementar soluciones de detección y respuesta ante amenazas (EDR) en todos los endpoints.
   - Capacitar al personal en la identificación de correos electrónicos y enlaces sospechosos.
   - Aplicar segmentación de red para limitar el alcance de posibles infecciones.
   - Establecer y probar planes de recuperación ante desastres y continuidad operativa.

5. **RECOMENDACIONES:**
   - https://www.bleepingcomputer.com/news/security/mathworks-blames-ransomware-attack-for-ongoing-outages/

Arla Foods confirma ciberataque que interrumpe su producción y causa retrasos

Tipo de Ataque: Ciberataque disruptivo – Interrupción de operaciones industriales

Medio de Propagación: Intrusión en sistemas IT con impacto en procesos OT

1. PRODUCTOS AFECTADOS:

- Sistemas de TI y producción de **Arla Foods**
- Procesos logísticos y de distribución en plantas de procesamiento de alimentos.

2. RESUMEN:

Arla Foods, una de las mayores cooperativas lácteas de Europa, confirmó que fue víctima de un ciberataque que interrumpió sus operaciones de producción y causó retrasos en la distribución. El incidente, ocurrido a finales de mayo de 2025, afectó tanto los sistemas informáticos como los procesos industriales, lo que sugiere un impacto mixto en entornos IT y OT.

3. DETALLE:

La empresa informó que el ataque comprometió sus sistemas internos, lo que obligó a detener temporalmente algunas líneas de producción y afectó la capacidad de entrega de productos. Aunque Arla no ha revelado detalles técnicos sobre el tipo de ataque ni el grupo responsable, se sabe que el incidente tuvo un efecto directo en la cadena de suministro.

Arla Foods está trabajando con expertos en ciberseguridad y autoridades para investigar el incidente, restaurar los sistemas afectados y garantizar la seguridad de sus operaciones. La empresa también ha comunicado que está tomando medidas para reforzar su infraestructura digital y prevenir futuros ataques.

Este caso resalta la vulnerabilidad de la industria alimentaria frente a ciberataques que pueden tener consecuencias operativas y económicas significativas.

4. RECOMENDACIONES:

- Implementar segmentación entre redes IT y OT para limitar el impacto cruzado.
- Fortalecer la ciberseguridad en entornos industriales con monitoreo en tiempo real.
- Realizar auditorías de seguridad y pruebas de penetración en sistemas críticos.
- Establecer planes de continuidad operativa y recuperación ante desastres.
- Capacitar al personal en protocolos de respuesta ante incidentes cibernéticos.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/arla-foods-confirms-cyberattack-disrupts-production-causes-delays/

China vinculada a ciberataques contra el sector de drones mediante compromisos en la cadena de suministro

Tipo de Ataque: Ciberespionaje estatal – Ataques a la cadena de suministro

Medio de Propagación: Campañas dirigidas con malware personalizado y explotación de proveedores comprometidos

1. PRODUCTOS AFECTADOS:

- Proveedores y socios tecnológicos vinculados a la cadena de suministro de drones

2. RESUMEN:

Investigadores de Trend Micro identificaron una serie de ataques cibernéticos dirigidos por un grupo vinculado a China, conocido como **Earth Ammit**, que comprometió la cadena de suministro del sector de drones en Asia Oriental. Las campañas, desarrolladas entre 2023 y 2024, afectaron a múltiples organizaciones en Taiwán y Corea del Sur, y se sospecha que forman parte de una estrategia más amplia de ciberespionaje industrial.

3. DETALLE:

El grupo Earth Ammit, asociado con actores de amenazas persistentes avanzadas (APT) chinos, llevó a cabo dos campañas de ataque diferenciadas. En la primera, se infiltraron en empresas proveedoras clave del ecosistema de drones, utilizando malware personalizado para comprometer sistemas internos. En la segunda ola, aprovecharon el acceso obtenido para atacar directamente a fabricantes y operadores de drones.

Los atacantes emplearon técnicas avanzadas de ingeniería social y herramientas de acceso remoto para mantener la persistencia en los sistemas comprometidos. El objetivo principal parece haber sido la obtención de información técnica sensible y la interrupción de operaciones estratégicas en el sector de defensa y tecnología.

Este tipo de ataques a la cadena de suministro representa una amenaza significativa, ya que permite a los atacantes infiltrarse en múltiples objetivos a través de un solo punto vulnerable, dificultando la detección y respuesta oportuna.

4. RECOMENDACIONES:

- Realizar evaluaciones de seguridad exhaustivas a proveedores y socios tecnológicos.
- Implementar controles de seguridad en toda la cadena de suministro, incluyendo autenticación multifactor y monitoreo continuo.
- Establecer protocolos de respuesta ante incidentes que incluyan a terceros.
- Capacitar al personal en la detección de técnicas de ingeniería social y phishing.
- Colaborar con agencias de inteligencia y ciberseguridad para compartir indicadores de compromiso (IoCs) y tácticas de ataque.

5. REFERENCIAS:

- https://www.securityweek.com/chinese-hackers-hit-drone-sector-in-supply-chain-attacks/

Masimo confirma ciberataque que afecta sus instalaciones de manufactura

Tipo de Ataque: Ciberataque a infraestructura IT con impacto en operaciones OT

Medio de Propagación: Acceso no autorizado a la red corporativa (vector no especificado públicamente)

6. PRODUCTOS AFECTADOS:

- Infraestructura de manufactura de **Masimo Corporation**
- Sistemas de TI corporativos
- Posible impacto en la producción de dispositivos médicos y electrónicos de consumo

7. RESUMEN:

Masimo Corporation, empresa tecnológica especializada en dispositivos médicos y electrónicos de consumo, confirmó que fue víctima de un ciberataque que afectó sus instalaciones de manufactura. El incidente fue detectado el 27 de abril de 2025 y reportado posteriormente a la Comisión de Bolsa y Valores de EE. UU. (SEC). La compañía está evaluando el impacto operativo y financiero del ataque.

8. DETALLE:

Según el comunicado oficial, el ataque comprometió la red interna de Masimo, lo que obligó a la empresa a tomar medidas de contención que incluyeron la interrupción temporal de ciertas operaciones de manufactura. Aunque no se han revelado detalles técnicos sobre el tipo de ataque ni sobre los actores responsables, la empresa indicó que está trabajando con expertos en ciberseguridad para investigar el incidente y restaurar completamente sus sistemas.

Masimo también señaló que está evaluando si se produjo alguna filtración de datos sensibles, aunque hasta el momento no se ha confirmado la exposición de información de clientes o empleados.

Este incidente resalta los riesgos que enfrentan las empresas del sector salud y tecnología cuando sus operaciones dependen de sistemas digitales interconectados.

9. RECOMENDACIONES:

- Implementar segmentación entre redes IT y OT para limitar el impacto cruzado.
- Fortalecer la seguridad de redes industriales con monitoreo en tiempo real y control de accesos.
- Realizar auditorías de seguridad periódicas y simulacros de respuesta ante incidentes.
- Establecer planes de continuidad operativa y recuperación ante desastres.
- Colaborar con autoridades y expertos externos para investigar y mitigar el impacto del ataque.

10. REFERENCIAS:

- https://www.securityweek.com/masimo-manufacturing-facilities-hit-by-cyberattack/