Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Julio - 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 Julio.

Alertas de Seguridad IT:

- Ataque de Ransomware SafePay interrumpe operaciones de Ingram Micro
- Filtraciones de datos en múltiples regiones afectan a Louis Vuitton
- Qantas, aerolínea nacional de Australia, confirma filtración de datos que afecta a 5.7 millones de clientes

Alertas de Seguridad OT/ICS:

- Ciberataque interrumpe medidores inteligentes de la principal empresa de servicios eléctricos de Nueva Escocia, Nova Scotia Power
- Clorox demanda a Cognizant tras ciberataque que costó 380 millones de dólares
- Vulnerabilidades críticas exponen routers industriales Helmholz a ciberataques

Ataque de Ransomware SafePay interrumpe operaciones de Ingram Micro

Tipo de Ataque: Ransomware

Medio de Propagación: Red Interna

1. **PRODUCTOS AFECTADOS:**
   - Sistemas internos de Ingram Micro
   - Infraestructura de TI corporativa
   - Servicios de soporte y operaciones logísticas

2. **RESUMEN:**

El proveedor global de soluciones tecnológicas Ingram Micro sufrió una interrupción significativa en sus operaciones debido a un ataque de ransomware atribuido al grupo SafePay. El incidente obligó a la compañía a desconectar varios sistemas internos como medida de contención. La interrupción afectó tanto a empleados como a clientes, generando demoras en servicios y operaciones logísticas.

3. **DETALLE:**

El ataque fue ejecutado por el grupo de ransomware SafePay, conocido por cifrar datos críticos y exigir rescates a cambio de la restauración del acceso. En este caso, los atacantes lograron comprometer la red interna de Ingram Micro, lo que sugiere una posible explotación de vulnerabilidades en servicios expuestos o credenciales comprometidas. Como respuesta, la empresa desconectó proactivamente sus sistemas para evitar una mayor propagación del malware. Aunque no se ha confirmado el vector inicial, se presume que el ataque pudo haberse originado a través de accesos remotos o correos electrónicos maliciosos. La compañía está trabajando con expertos en ciberseguridad para contener el incidente y restaurar sus servicios.

4. **RECOMENDACIONES:**
   - Implementar soluciones de respaldo y recuperación ante desastres.
   - Actualizar todos los sistemas y aplicaciones con los últimos parches de seguridad.
   - Restringir el acceso remoto mediante autenticación multifactor (MFA).
   - Monitorear continuamente la red en busca de actividades sospechosas.
   - Capacitar al personal en la identificación de correos electrónicos de phishing.
   - Realizar auditorías periódicas de seguridad en la infraestructura crítica.

5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/ingram-micro-outage-caused-by-safepay-ransomware-attack/

Filtraciones de datos en múltiples regiones afectan a Louis Vuitton

Tipo de Ataque: **Exposición de Información**

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

1. **PRODUCTOS AFECTADOS:**
   - Portales de clientes de Louis Vuitton en Corea del Sur, Turquía y Reino Unido
   - Bases de datos regionales de clientes
   - Sistemas de notificación y gestión de cuentas

2. **RESUMEN:**

Louis Vuitton ha confirmado que varias filtraciones de datos ocurridas en distintas regiones están relacionadas con un mismo ciberataque. Las brechas afectaron inicialmente a Corea del Sur, luego a Turquía y más recientemente al Reino Unido. En todos los casos, se notificó a los clientes sobre la exposición de su información personal. La empresa está investigando el incidente y ha implementado medidas de contención.

3. **DETALLE**

El incidente se originó a partir de un acceso no autorizado a sistemas regionales de Louis Vuitton, lo que permitió a los atacantes extraer información personal de clientes, incluyendo nombres, direcciones y detalles de contacto. Aunque no se ha revelado el vector exacto del ataque, la simultaneidad y similitud de las brechas sugiere una vulnerabilidad común explotada en múltiples entornos regionales. La compañía está trabajando con expertos en ciberseguridad para identificar el origen del ataque, contener su propagación y reforzar sus defensas. Hasta el momento, no se ha confirmado la participación de un grupo específico ni se ha reportado el uso de ransomware.

4. **RECOMENDACIONES:**
   - Revisar configuraciones de seguridad en sistemas regionales y portales web.
   - Implementar monitoreo centralizado de accesos y actividades sospechosas.
   - Actualizar credenciales y aplicar autenticación multifactor en todos los accesos administrativos.
   - Notificar a los usuarios afectados y ofrecer medidas de protección de identidad.
   - Auditar la infraestructura para detectar vulnerabilidades comunes entre regiones.
   - Limitar el acceso a datos sensibles según el principio de privilegio mínimo.

5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/louis-vuitton-says-regional-data-breaches-tied-to-same-cyberattack/

Qantas, aerolínea nacional de Australia, confirma filtración de datos que afecta a 5.7 millones de clientes

Tipo de Ataque: Exposición de Información
Medio de Propagación: Acceso no autorizado a sistemas internos

1. **PRODUCTOS AFECTADOS:**
   - In Aplicación móvil Qantas Frequent Flyer
   - Plataforma de fidelización de clientes
   - Bases de datos de clientes registrados

2. **RESUMEN:**

La aerolínea australiana Qantas ha confirmado una filtración de datos que afecta a aproximadamente 5.7 millones de clientes. El incidente fue detectado tras una revisión interna que reveló accesos no autorizados a información personal almacenada en su plataforma de fidelización. La compañía ha iniciado una investigación y está notificando a los usuarios afectados.

3. **DETALLE:**

El ataque comprometió datos personales de clientes registrados en el programa Qantas Frequent Flyer, incluyendo nombres, direcciones de correo electrónico, números de membresía y detalles de vuelos. Aunque no se ha confirmado el método exacto de intrusión, se presume que los atacantes explotaron vulnerabilidades en la aplicación móvil o en los sistemas de autenticación. Qantas ha indicado que no se expusieron contraseñas ni información financiera, pero ha reforzado sus controles de seguridad y está colaborando con autoridades regulatorias para mitigar el impacto.

4. **RECOMENDACIONES:**
   - Revisar los registros de acceso y actividad en plataformas móviles y web.
   - Actualizar las políticas de autenticación y aplicar MFA en todos los accesos sensibles.
   - Notificar a los usuarios afectados y ofrecer orientación sobre medidas de protección.
   - Implementar monitoreo continuo de seguridad en aplicaciones móviles.
   - Auditar las integraciones de terceros y servicios conectados a la plataforma de fidelización.
   - Limitar el acceso a datos personales según el principio de privilegio mínimo.

5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/qantas-confirms-data-breach-impacts-57-million-customers/

Ciberataque interrumpe medidores inteligentes de la principal empresa de servicios eléctricos de Nueva Escocia, Nova Scotia Power

Tipo de Ataque: Interrupción de Servicios - Ciberataque dirigido

Medio de Propagación: Red Interna

1. PRODUCTOS AFECTADOS:

- Medidores inteligentes de Nova Scotia Power
- Infraestructura de monitoreo y control de energía
- Sistemas de comunicación con clientes

2. RESUMEN:

La empresa canadiense Nova Scotia Power confirmó que un ciberataque afectó el funcionamiento de sus medidores inteligentes, generando interrupciones en la recolección de datos de consumo eléctrico. El incidente también impactó a algunos usuarios en Estados Unidos. La compañía está trabajando con expertos en ciberseguridad y autoridades para contener el ataque y restaurar los servicios afectados.

3. DETALLE:

El ataque comprometió la infraestructura digital que gestiona los medidores inteligentes, interrumpiendo la transmisión de datos entre los dispositivos y los sistemas centrales de Nova Scotia Power. Aunque no se ha revelado el vector exacto del ataque ni el grupo responsable, se presume que los atacantes accedieron a la red interna de la empresa, posiblemente mediante vulnerabilidades en sistemas de control industrial (ICS) o mediante accesos remotos no seguros. La empresa ha iniciado una investigación forense y ha reforzado sus medidas de seguridad para evitar futuras intrusiones.

4. RECOMENDACIONES:

- Aislar los sistemas críticos de control industrial de redes externas.
- Actualizar firmware y software de medidores inteligentes y sistemas de monitoreo.
- Implementar segmentación de red para limitar la propagación de amenazas.
- Monitorear continuamente la infraestructura crítica en busca de anomalías.
- Revisar y fortalecer los controles de acceso remoto y autenticación.
- Coordinar con autoridades nacionales para compartir indicadores de compromiso (IoC).

5. REFERENCIAS:

- https://www.securityweek.com/canadian-electric-utility-says-power-meters-disrupted-by-cyberattack/

Clorox demanda a Cognizant tras ciberataque que costó 380 millones de dólares

Tipo de Ataque: Ingeniería Social

Medio de Propagación: Llamada telefónica fraudulenta al soporte técnico

1. **PRODUCTOS AFECTADOS:**
   - Infraestructura de TI de Clorox
   - Cuentas de usuario con privilegios
   - Sistemas de producción y distribución
2. **RESUMEN:**

Clorox ha presentado una demanda contra Cognizant, su proveedor de servicios TI, alegando que un ciberataque devastador fue posible debido a una falla en los protocolos de autenticación del soporte técnico. Los atacantes engañaron al help desk de Cognizant para obtener acceso a las credenciales de un empleado de Clorox, lo que resultó en una interrupción operativa con pérdidas estimadas en 380 millones de dólares.

3. **DETALLE:**

El ataque se basó en una táctica de ingeniería social conocida como vishing, en la que los atacantes se hicieron pasar por un empleado legítimo de Clorox y contactaron al help desk de Cognizant. Debido a la falta de verificación de identidad robusta, el personal de soporte restableció las credenciales de acceso sin confirmar adecuadamente la identidad del solicitante. Con las nuevas credenciales, los atacantes accedieron a la red interna de Clorox, donde desplegaron malware que afectó múltiples sistemas, incluyendo los de manufactura, distribución y ventas. La falta de segmentación de red y controles de acceso granulares permitió a los atacantes moverse lateralmente dentro del entorno corporativo. La demanda de Clorox argumenta que Cognizant incumplió sus obligaciones contractuales al no aplicar controles de seguridad adecuados, lo que facilitó el acceso no autorizado y amplificó el impacto del ataque.

4. **RECOMENDACIONES:**
   - Implementar protocolos estrictos de verificación de identidad en centros de soporte.
   - Capacitar al personal de TI en detección de intentos de ingeniería social.
   - Restringir el restablecimiento de credenciales a través de canales no verificados.
   - Auditar los procedimientos de soporte técnico de terceros.
   - Aplicar autenticación multifactor obligatoria para accesos privilegiados.
   - Monitorear continuamente los accesos y actividades sospechosas en cuentas críticas.

5. **REFERENCIAS:**

- https://www.bleepingcomputer.com/news/security/hackers-fooled-cognizant-help-desk-says-clorox-in-380m-cyberattack-lawsuit/

Vulnerabilidades críticas exponen routers industriales Helmholz a ciberataques

Tipo de Ataque: Explotación de Vulnerabilidades / Acceso Remoto No Autorizado

Medio de Propagación: Red Interna / Acceso remoto a dispositivos expuestos

6. PRODUCTOS AFECTADOS:

- Routers industriales Helmholz REX 100
- Infraestructura de redes industriales (OT)
- Sistemas conectados a través de los routers comprometidos

7. RESUMEN:

Se han identificado múltiples vulnerabilidades críticas en los routers industriales Helmholz REX 100, ampliamente utilizados en entornos de automatización. Estas fallas permiten a atacantes obtener control total sobre los dispositivos, comprometiendo la seguridad de redes industriales. Las vulnerabilidades ya han sido corregidas por el fabricante, pero los dispositivos sin actualizar siguen expuestos.

8. DETALLE:

Investigadores descubrieron varias vulnerabilidades en el firmware de los routers Helmholz REX 100, incluyendo fallas de autenticación insuficiente, ejecución remota de comandos y exposición de credenciales. Una de las vulnerabilidades más graves permite a un atacante autenticarse sin credenciales válidas y ejecutar comandos arbitrarios con privilegios elevados, lo que facilita el control total del dispositivo.Además, se detectaron configuraciones inseguras que permiten el acceso remoto a interfaces administrativas sin cifrado, exponiendo los routers a interceptación de tráfico y manipulación. Estas debilidades representan un riesgo significativo en entornos industriales, donde los routers actúan como puente entre redes OT y sistemas corporativos. Un atacante que comprometa estos dispositivos podría alterar procesos industriales, interrumpir operaciones o moverse lateralmente hacia otros sistemas críticos. El fabricante ha lanzado actualizaciones de firmware que corrigen estas fallas, pero se advierte que muchos dispositivos aún operan con versiones vulnerables, especialmente en instalaciones donde el mantenimiento de seguridad no es frecuente.

9. RECOMENDACIONES:

- Actualizar inmediatamente el firmware de los routers Helmholz REX 100 a la última versión disponible y deshabilitar el acceso remoto a interfaces administrativas si no es estrictamente necesario.
- Segmentar las redes industriales para limitar el alcance de posibles intrusiones y aplicar MFA donde sea posible.

10. REFERENCIAS:

- https://www.securityweek.com/vulnerabilities-expose-helmholz-industrial-routers-to-hacking/