Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Abril - 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:

- Hackeo paraliza los sistemas del INTA: suspenden servicios y reportes técnicos
- Hitachi Vantara desconecta servidores tras ataque de ransomware Akira
- Uso indebido de accesos del Mininter expone fotografías de 25 millones de peruanos

Alertas de Seguridad OT/ICS:

- Vulnerabilidad en firewall de Palo Alto afecta producto industrial de Siemens
- Sensata Technologies sufre ataque de ransomware que interrumpe operaciones
- China admite su implicación en ciberataques contra infraestructura crítica de EE. UU.

Hackeo paraliza los sistemas del INTA: suspenden servicios y reportes técnicos

Tipo de Ataque: Hackeo informático

Medio de Propagación: Redes internas de INTA

1. **PRODUCTOS AFECTADOS:**
   - Red de servidores del Instituto Nacional de Tecnología Agropecuaria (INTA)

2. **RESUMEN:**

El Instituto Nacional de Tecnología Agropecuaria (INTA) fue blanco de un ataque informático que dejó fuera de servicio parte de su red de servidores y afectó el funcionamiento normal de sus dependencias. El ataque obligó a desconectar equipos y suspender actividades clave, afectando la emisión de reportes técnicos y otros servicios esenciales

3. **DETALLE:**

El incidente comenzó a ser reportado internamente en la mañana del martes 15 de abril de 2025, y ya el miércoles se notificó oficialmente la interrupción de algunos servicios. Los trabajadores del INTA confirmaron que no podían acceder a dominios como Inta.gob.ar y que las máquinas debían ser desconectadas de la red. El último informe agrometeorológico, que se actualiza semanalmente, fue el publicado el 8 de abril, lo que indica una interrupción significativa en la actualización de datos cruciales. El ataque afectó seriamente las operaciones del organismo, que continúa trabajando para contener el daño y restablecer sus sistemas.

4. **RECOMENDACIONES:**
   - Reforzar las medidas de seguridad de la red interna con sistemas de detección de intrusiones y firewalls avanzados.
   - Actualizar y parchear regularmente todos los sistemas y aplicaciones para prevenir vulnerabilidades.
   - Implementar una estrategia de copias de seguridad periódicas y asegurar su integridad.
   - Realizar capacitaciones periódicas en seguridad cibernética para todo el personal.
   - Desarrollar un plan de respuesta a incidentes y asegurar un equipo especializado disponible.
   - Colaborar con autoridades locales y organismos de ciberseguridad para investigar y prevenir ataques.
   - Implementar soluciones de monitoreo y auditorías regulares para detectar patrones inusuales.

5. **REFERENCIAS:**
   - https://www.ellitoral.com.ar/sociedad/2025-4-16-18-54-0-hackeo-paraliza-los-sistemas-del-inta-suspenden-servicios-y-reportes-tecnicos

Hitachi Vantara desconecta servidores tras ataque de ransomware Akira

Tipo de Ataque: Ransomware

Medio de Propagación: No confirmado oficialmente. Sin embargo, se sabe que el grupo Akira ha utilizado métodos como explotación de vulnerabilidades en VPNs, accesos remotos no autorizados y correos electrónicos de phishing en ataques anteriores.

1. **PRODUCTOS AFECTADOS:**
   - Servidores internos de Hitachi Vantara

2. **RESUMEN:**

Hitachi Vantara, una subsidiaria del conglomerado japonés Hitachi, que se enfoca en soluciones de infraestructura de datos, análisis y gestión de datos, y servicios de nube híbrida, fue víctima de un ataque de ransomware por parte del grupo Akira. El ataque obligó a la empresa a desconectar varios servidores para contener la propagación del ransomware y minimizar el daño.

3. **DETALLE**

El ataque ocurrió el 26 de abril de 2025, causando interrupciones significativas en los sistemas de la empresa. Hitachi Vantara detectó actividades sospechosas y activó sus protocolos de respuesta a incidentes, desconectando servidores para limitar el impacto. La empresa ha contratado a expertos en ciberseguridad para investigar y recuperar los sistemas afectados. Aunque los servicios en la nube de Hitachi Vantara no se vieron afectados, los sistemas internos y los entornos de producción sí lo fueron. El grupo Akira es conocido por exfiltrar datos sensibles y dejar notas de rescate en los sistemas infectados. El ataque también afectó varios proyectos gubernamentales, destacando la gravedad y los riesgos potenciales a nivel nacional. Akira, que emergió en marzo de 2023, ha comprometido a más de 300 organizaciones en todo el mundo, con demandas de rescate que varían entre $200,000 y varios millones de dólares. Según el FBI, Akira ha recaudado aproximadamente $42 millones en pagos de rescate hasta abril de 2024.

4. **RECOMENDACIONES:**
   - Priorizar controles de acceso sólidos y actualizaciones periódicas del sistema para mitigar el riesgo de ataques de ransomware.
   - Configurar la segmentación de la red para limitar la propagación de malware y realizar programas de capacitación y concientización de los usuarios.
   - Implementar soluciones de seguridad proactiva, como plataformas impulsadas por IA, para brindar protección integral al predecir y prevenir amenazas.
   - Mantenerse informado sobre los indicadores de compromiso (IoC) y aprovechar la inteligencia sobre amenazas para mantener defensas de ciberseguridad efectivas.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/hitachi-vantara-takes-servers-offline-after-akira-ransomware-attack/

Uso indebido de accesos del Mininter expone fotografías de 25 millones de peruanos

Tipo de Ataque: **Insider Attack – Data Breach**

Medio de Propagación: **Foro clandestino de internet- Breachforums**

1. **PRODUCTOS AFECTADOS:**
   - Datos personales y fotografías de ciudadanos peruanos

2. **RESUMEN:**

Un ciberdelincuente conocido como "Gatito_FBI_NZ" accedió a las fotografías de 25 millones de peruanos alojadas en los servidores del Reniec. El atacante está ofreciendo la información privada en el foro Breachforums.

3. **DETALLE**

El incidente ocurrió debido al uso indebido de un servicio de consultas en línea autorizado por el Reniec al Ministerio del Interior (Mininter) para cumplir funciones oficiales. A través de este acceso legítimo, un usuario del Mininter habría extraído de forma no autorizada información sensible, incluyendo fotografías de ciudadanos peruanos.

A inicios de marzo, al detectar un uso irregular del sistema, el Reniec suspendió inmediatamente el acceso del Mininter. La entidad también presentó una denuncia formal ante la Fiscalía de la Nación y la Autoridad Nacional de Protección de Datos Personales, además de notificar a la Presidencia del Consejo de Ministros (PCM) y a la Secretaría de Gobierno y Transformación Digital (SGTD).

El 2 de abril, un ciberdelincuente identificado como "Gatito_FBI_NZ" publicó en el foro clandestino Breachforums que poseía las fotografías de 25 millones de peruanos, y comenzó a ofertarlas por USD 300. Como muestra, entregó más de 140 mil imágenes que contenían marcas de agua del Reniec, Mininter y del DNI del usuario que accedió a la base de datos. El atacante afirmó que entregaría los 10 millones restantes tras la venta del primer paquete de 15 millones.

Cabe destacar que el Reniec ha negado que sus sistemas hayan sido directamente vulnerados, señalando que la filtración se produjo por el mal uso de accesos autorizados, y no por un ataque externo a sus servidores.

4. **RECOMENDACIONES:**
   - **Fortalecer la seguridad de los servidores:** Implementar medidas de seguridad avanzadas para proteger los servidores del Reniec y del Mininter contra ataques informáticos.
   - **Encriptación de datos:** Asegurar que todos los datos sensibles estén encriptados para dificultar el acceso y la utilización por parte de ciberdelincuentes.
   - **Monitoreo y detección de amenazas:** Utilizar herramientas de monitoreo continuo para detectar y responder rápidamente a cualquier actividad sospechosa.
   - **Respuesta a incidentes:** Desarrollar y mantener un plan de respuesta a incidentes que permita actuar rápidamente en caso de un ataque.

- **Colaboración con autoridades:** Trabajar estrechamente con las autoridades para investigar el ataque y tomar medidas legales contra los responsables.
- **Capacitación y concientización**: Implementar programas de capacitación y concientización para el personal que maneje información sensible en el Mininter, enfocándose en el uso adecuado y seguro de los datos.

5. REFERENCIAS:

- https://www.infobae.com/peru/2025/04/04/reniec-niega-hackeo-masivo-y-denuncia-al-mininter-como-responsable-del-uso-indebido-de-datos/
- https://elfoco.pe/2025/04/rafagas/atacan-servidores-del-reniec-y-mininter-y-filtran-fotografias-de-25-millones-de-peruanos/

Vulnerabilidad en firewall de Palo Alto afecta producto industrial de Siemens

Tipo de Ataque: Zero-Day Exploit – Remote Command Execution

Medio de Propagación: Vulnerabilidad en dispositivos expuestos a internet (CVE-2024-3400)

1. PRODUCTOS AFECTADOS:

- Siemens Ruggedcom APE1808 (cuando se encuentra configurado con un firewall virtual de Palo Alto Networks)

2. RESUMEN:

Una grave vulnerabilidad en los firewalls de Palo Alto Networks (CVE-2024-3400), explotada como día cero, también afecta a los dispositivos industriales Siemens Ruggedcom APE1808. Siemens confirmó el impacto y ha publicado medidas de mitigación mientras prepara una actualización de seguridad. La falla permite a atacantes ejecutar comandos arbitrarios con privilegios elevados, y ya ha sido explotada en entornos reales, aunque no se ha confirmado que los dispositivos Siemens hayan sido blanco directo.

3. DETALLE:

CVE-2024-3400 es una vulnerabilidad crítica en los firewalls de Palo Alto Networks que permite a atacantes no autenticados ejecutar comandos con privilegios elevados. Esta falla ha sido activamente explotada desde al menos marzo de 2024, incluso antes de que existieran parches o mitigaciones oficiales, lo que la clasifica como una vulnerabilidad de día cero.

Siemens informó que su plataforma Ruggedcom APE1808 —utilizada para aplicaciones de ciberseguridad en entornos industriales hostiles— podría verse afectada si está configurada con un firewall virtual de Palo Alto Networks. Aunque Siemens no ha reportado ataques dirigidos específicamente a su producto, la compañía ha emitido recomendaciones provisionales y está desarrollando actualizaciones.

Actualmente, aproximadamente 6,000 dispositivos Palo Alto expuestos a internet continúan siendo vulnerables. Se sospecha que los primeros ataques podrían estar vinculados a un actor estatal, posiblemente relacionado con el grupo Lazarus de Corea del Norte, aunque esta relación no ha sido confirmada. Según Volexity, los atacantes habrían comenzado a explotar la vulnerabilidad el 26 de marzo, accediendo a redes internas, exfiltrando datos y, en algunos casos, instalando puertas traseras.

4. RECOMENDACIONES:

- Aplicar de inmediato las mitigaciones temporales provistas por Siemens y/o Palo Alto.
- Actualizar los dispositivos afectados tan pronto como se liberen los parches.
- Limitar la exposición de firewalls a internet siempre que sea posible.
- Supervisar redes industriales para detectar actividad sospechosa.
- Evaluar el uso de soluciones de detección de intrusos (IDS/IPS) específicas para entornos OT.
- Seguir las publicaciones de seguridad oficiales de Siemens para nuevas actualizaciones.

5. REFERENCIAS:

- https://www.securityweek.com/siemens-industrial-product-impacted-by-exploited-palo-alto-firewall-vulnerability/

Sensata Technologies sufre ataque de ransomware que interrumpe operaciones

Tipo de Ataque: Ransomware

Medio de Propagación: Red interna de Sensata Technologies

1. PRODUCTOS AFECTADOS:

- Sistemas internos de Sensata Technologies, incluyendo producción, envío, recepción y funciones de soporte.

2. RESUMEN:

Sensata Technologies, especializada en sensores y controles para los sectores automotriz, aeroespacial y manufacturero, fue víctima de un ataque de ransomware que cifró dispositivos en su red interna. El incidente interrumpió temporalmente varias operaciones de la empresa, incluyendo producción, envío, recepción y funciones de soporte. La compañía implementó medidas provisionales para restaurar ciertas funciones, aunque el tiempo estimado para una restauración completa aún no se conoce.

3. DETALLE:

El ataque comenzó a finales de la semana anterior al anuncio público. Sensata Technologies reportó que varios de sus sistemas internos fueron cifrados por el ransomware, afectando así su infraestructura crítica. Aunque los detalles específicos del tipo de ransomware aún no se han divulgado, el ataque interrumpió de inmediato varias de sus operaciones diarias, incluyendo la capacidad de enviar productos a clientes y recibir materiales esenciales.

Acciones Tomadas:

- **Contención Inmediata:** Tras detectar el ataque, Sensata desconectó partes de su red interna para limitar la propagación del ransomware.
- **Investigación en curso:** La compañía contrató a expertos en ciberseguridad para investigar a fondo el incidente y determinar el alcance del ataque. Esto incluye la identificación de los sistemas afectados y los posibles daños en datos o información sensible.
- **Restauración de Sistemas:** Aunque algunos sistemas han sido restaurados, se desconoce la extensión del tiempo necesario para que la operación vuelva a la normalidad en su totalidad.
- **Notificación a las Autoridades:** Sensata ha informado a las autoridades competentes y está siguiendo los procedimientos legales establecidos para tratar con este tipo de incidentes.
- **Impacto Financiero:** En cuanto al impacto financiero, Sensata no anticipa que este ataque afecte significativamente sus resultados financieros durante el trimestre en curso, pero aún están en proceso de evaluar los daños a largo plazo.

No se ha confirmado si el ransomware fue entregado a través de un ataque de phishing, vulnerabilidades de software u otro método. Sin embargo, el incidente subraya la importancia de las medidas de ciberseguridad avanzadas y la necesidad de una rápida respuesta ante tales amenazas.

Colaboración con Expertos:

Sensata ha estado colaborando estrechamente con expertos de ciberseguridad externos para mitigar el daño y fortalecer sus defensas. Aunque la empresa aún no ha revelado si los atacantes han solicitado un rescate, la información sobre la amenaza sigue siendo limitada.

4. RECOMENDACIONES:

- Se recomienda a las organizaciones implementar medidas de protección como firewalls avanzados, sistemas de detección de intrusiones y plataformas de inteligencia de amenazas para prevenir estos ataques.
- Asegurar que todas las copias de seguridad sean almacenadas en lugares aislados y que se mantengan actualizadas, de modo que puedan ser recuperadas rápidamente en caso de un ataque.
- Capacitar a los empleados con campañas de phishing y otros métodos de ataque comunes, lo que puede ser crucial para evitar la infiltración de malware.
- Desarrollar y probar un plan de respuesta a incidentes para poder actuar rápidamente si se presenta un ataque de ransomware u otra amenaza cibernética.
- Trabajar con expertos en ciberseguridad para monitorear continuamente las vulnerabilidades y fortalecer las defensas.

5. REFERENCIAS:

- https://www.cybersecuritydive.com/news/sensata-technologies-disrupted-ransomware-attack/745007/

China admite su implicación en ciberataques contra infraestructura crítica de EE. UU.

Tipo de Ataque: Ciberespionaje estatal – Campaña de acceso persistente (APT)

Medio de Propagación: Campaña de intrusión "Volt Typhoon" mediante técnicas de "living-off-the-land"

1. **PRODUCTOS AFECTADOS:**
   - Infraestructura crítica de EE. UU., incluyendo puertos, servicios de agua, aeropuertos y redes de telecomunicaciones
2. **RESUMEN:**

En una reunión secreta celebrada en diciembre de 2024 en Ginebra, funcionarios chinos reconocieron implícitamente su responsabilidad en una serie de ciberataques sofisticados contra infraestructuras críticas de EE. UU. Estos ataques, atribuidos a la campaña conocida como "Volt Typhoon", fueron interpretados por la delegación estadounidense como una advertencia relacionada con el apoyo de EE. UU. a Taiwán.

3. **DETALLE:**

Durante una cumbre confidencial en Ginebra, representantes del Ministerio de Asuntos Exteriores de China, incluyendo al alto funcionario cibernético Wang Lei, discutieron con funcionarios estadounidenses sobre las intrusiones en redes críticas de EE. UU. Aunque no hubo una admisión explícita, los comentarios fueron interpretados como una confirmación tácita de la implicación de Pekín en los ataques. La campaña "Volt Typhoon" ha sido descrita por expertos en seguridad como una operación de ciberespionaje altamente sofisticada, que utiliza técnicas de "living-off-the-land" para evitar la detección y mantener el acceso persistente a las redes comprometidas. Estas técnicas incluyen el uso de herramientas legítimas del sistema para ejecutar comandos maliciosos sin levantar sospechas.

Los ataques se centraron en infraestructuras civiles críticas, lo que representa una escalada en las tácticas de ciberespionaje y plantea preocupaciones sobre la preparación para posibles conflictos futuros. La admisión, aunque indirecta, marca un cambio significativo en la postura de China, que anteriormente negaba cualquier implicación en actividades cibernéticas maliciosas.

4. **RECOMENDACIONES:**
   - Fortalecer las defensas cibernéticas en infraestructuras críticas mediante la implementación de sistemas de detección y respuesta ante intrusiones (IDR).
   - Actualizar y parchear regularmente los sistemas para mitigar vulnerabilidades conocidas.
   - Implementar segmentación de redes y políticas de mínimo privilegio para limitar el movimiento lateral de atacantes.
   - Realizar auditorías de seguridad y simulacros de respuesta ante incidentes para mejorar la preparación organizacional.
   - Colaborar con agencias gubernamentales y compartir información sobre amenazas para una respuesta coordinada.

5. REFERENCIAS:

- https://cybersecuritynews.com/china-reportedly-admits-their-role-in-cyber-attacks/