Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Noviembre - 2024

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 septiembre.

Alertas de Seguridad IT:

- Starbucks sufre un ataque de ransomware a través de un proveedor de software externo
- Red hospitalaria del Reino Unido pospone procedimientos tras ciberataque
- Hackers chinos violaron los enrutadores de T-Mobile para explorar la red

Alertas de Seguridad OT/ICS:

- Schneider Electric lanza una investigación después de que piratas informáticos afirmaran haber robado datos de sus usuarios
- Seguridad ICS: 145.000 sistemas expuestos a la Web, numerosas empresas industriales afectadas por ataques

Starbucks sufre un ataque de ransomware a través de un proveedor de software externo

Tipo de Ataque: **Ransomware y Disrupción Operativa**

Medio de Propagación: **Vulnerabilidades en la cadena de suministro de software**

1. **PRODUCTOS AFECTADOS:**
   - Software de gestión de la cadena de suministro de software
   - Sistemas de programación y nómina de Starbucks

2. **RESUMEN:**

Un ataque de ransomware a Blue Yonder, proveedor líder de software para la gestión de la cadena de suministro, ha causado interrupciones significativas en los sistemas de Starbucks, obligando a la empresa a recurrir a procesos manuales para la programación de horarios y la gestión de nóminas. Aunque el incidente no ha afectado el servicio al cliente, ha creado un impacto notable en la operatividad interna. Además, el ataque ha generado efectos colaterales en otros sectores, como el comercio minorista en el Reino Unido, donde cadenas como Morrisons y Sainsbury´s reportaron interrupciones en sus sistemas de gestión de almacenes. Blue Yonder, que presta servicios a algunos de los principales minoristas y fabricantes del mundo, ha contratado expertos externos en ciberseguridad para mitigar la situación, sin proporcionar un cronograma claro para la restauración del servicio.

3. **DETALLE:**

El ataque de ransomware, que comenzó el 21 de noviembre de 2024, evidenció la vulnerabilidad de los sistemas de la cadena de suministro en un periodo crítico como la temporada navideña. Gerentes de Starbucks se vieron obligados a recurrir a métodos manuales como lápiz y papel para registrar las horas trabajadas de los empleados, lo que ha generado desafíos administrativos. En el Reino Unido, los principales minoristas a nivel mundial, no ha comunicado un cronograma definitivo para solucionar el incidente. Este ataque subraya un patrón recurrente en el que el 86% de los ataques de ransomware apuntan a organizaciones durante días festivos o fines de semana, aprovechando las operaciones reducidas de seguridad.

4. **RECOMENDACIONES:**
   - Implementar sistemas de respaldo que permiten mantener operaciones críticas frente a interrupciones inesperadas.
   - Capacitar a los equipos internos en procedimientos de respuesta ante incidentes de ransomware, priorizando la continuidad operativa.
   - Establecer acuerdos con proveedores estratégicos que incluyan cláusulas específicas sobre ciberseguridad y protocolos de recuperación.
   - Monitorear continuamente la actividad de los sistemas críticos durante días festivos o periodos de alta actividad para identificar posibles amenazas.

5. **REFERENCIAS:**
   - https://cybersecuritynews.com/starbucks-hit-by-ransomware-attack/

Red hospitalaria del Reino Unido pospone procedimientos tras ciberataque

Tipo de Ataque: **Aún no identificado**

Medio de Propagación: **Actividad sospechosa en sistemas de TI**

1. **PRODUCTOS AFECTADOS:**
   - Registros médicos electrónicos
   - Sistemas de diagnóstico y resultados
   - Programación de citas y procedimientos

2. **RESUMEN:**

El WUTH, parte del NHS Foundation Trust en el Reino Unido, sufrió un ciberataque significativo que obligó a la desconexión de sistemas críticos de TI. Esta acción preventiva, tomada para contener la amenaza, ha llevado a retrasos e interrupciones en servicios hospitalarios esenciales, incluidos los de emergencia y cirugías programadas. El persona ha tenido que recurrir a procesos manuales, afectando la eficiencia operativa y aumentando los tiempos de espera para los pacientes. .

3. **DETALLE**

El ataque, detectado a principios de semana, activó medidas de contingencia en el hospital, incluyendo el uso de registros en papel. Los sistemas desconectados han dejado al personal sin acceso a historiales médicos, resultados de laboratorio y herramientas digitales de gestión. Esto ha obligado a reprogramar citas y procedimientos programados, mientras que los servicios de emergencia enfrentan mayores tiempos de espera. Aunque el ataque no ha sido atribuido a ningún grupo específico, el impacto es evidente: pacientes en Arrowe Park y otros hospitales asociados no tienen acceso a servicios como rayos X, tratamientos ni cirugías. Las autoridades del hospital han solicitado al público que evite acudir a urgencias a menos que sea estrictamente necesario para evitar una sobrecarga.

4. **RECOMENDACIONES:**
   - Implementar la segmentación de red para limitar la propagación de amenazas en caso de futuros ataques.
   - Capacitar al personal en protocolos de continuidad operativa y gestión de incidentes para asegurar una respuesta adecuada.
   - Realizar auditorías periódicas que permitan identificar y corregir vulnerabilidades en la infraestructura de TI.
   - Asegurar la existencia de copias de seguridad frecuentes y protegidas contra accesos no autorizados.
   - Diseñar procedimientos manuales de emergencia que sean eficientes y minimicen el impacto operativo en situaciones críticas.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/uk-hospital-network-postpones-procedures-after-cyberattack/

Hackers chinos violaron los enrutadores de T-Mobile para explorar la red

Tipo de Ataque: **Reconocimiento inicial y movimiento lateral (detenido)**
Medio de Propagación: **Enrutadores comprometidos dentro de la red de un proveedor de telefonía fija conectado.**

1. PRODUCTOS AFECTADOS:

- Enrutadores de red utilizados para telecomunicaciones
- Infraestructura interna de TI de T-Mobile

2. RESUMEN:

T-Mobile enfrentó un intento de ciberataque por parte del grupo chino patrocinado por el estado conocido como Salt Typhoon (también identificado como Earth Estries, FamousSparrow, Ghost Emperor, y UNC2286). Los atacantes inicialmente comprometieron enrutadores conectados para explotar formas de movimiento lateral dentro de la red. Sin embargo, las defensas proactivas de T-Mobile lograron contener la amenaza antes de que pudiera propagarse o acceder a datos sensibles de los clientes.

El incidente se detectó gracias al monitoreo activo que identificó comandos utilizados en la etapa de reconocimiento de ciberataques. La compañía asegura que no hubo acceso a información confidencial de los clientes ni interrupciones en los servicios.

3. DETALLE:

El ataque, detectado a través de comportamientos sospechosos en la red, incluyó comandos característicos de las etapas iniciales de ciberataques y coincidentes con indicadores asociados a Salt Typhoon. Los atacantes comprometieron la red de un proveedor externo conectado para explotar posibles vulnerabilidades dentro de T-Mobile.

4. RECOMENDACIONES:

- Fortalecer la segmentación de red para limitar accesos laterales en futuros compromisos.
- Implementar herramientas avanzadas de detección para identificar comportamientos anómalos en tiempo real.
- Capacitar a los equipos de TI y proveedores en protocolos de ciberseguridad.
- Realizar auditorías periódicas a la infraestructura de proveedores externos conectados.
- Mantener procedimientos de respuesta rápida para minimizar el impacto de futuras amenazas.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/chinese-hackers-breached-t-mobiles-routers-to-scope-out-network

Schneider Electric investiga una violación de datos confidenciales

Tipo de Ataque: Filtración de datos y Extorción
Medio de Propagación: Acceso no autorizado a plataformas internas de seguimiento de proyectos

5. PRODUCTOS AFECTADOS:

- Sistema Jira de seguimiento de problemas
- Bases de datos internas de Schneider Electric

6. RESUMEN:

Schneider Electric, el gigante industrial francés, ha iniciado una investigación tras la afirmación del grupo de hackers Hellcat de haber accedido a su sistema de seguimiento de problemas Jira. Los atacantes aseguran haber robado más de 40 GB de datos comprimidos, incluidos proyectos, problemas, complementos y más de 400,000 registros de usuarios. Exigen un rescate de $125,000, con una reducción del 50% si la compañía confirma la violación. Schneider Electric ha activado su equipo de Respuesta a Incidentes Globales para abordar el incidente, aclarando que sus productos y servicios no fueron comprometidos.

7. DETALLE:

El grupo Hellcat afirmó haber obtenido acceso completo al sistema Jira de Schneider Electric, compartiendo capturas de pantalla como evidencia en la red social X. Según los hackers, los datos incluyen información sensible de proyectos y usuarios. El incidente, alojado en un entorno aislado según Schneider, es el segundo ataque cibernético que sufre la empresa este año. Previamente, su división Sustainability Business fue víctima del grupo de ransomware Cactus.

8. RECOMENDACIONES:

- Revisar y reforzar las políticas de acceso y autenticación en sistemas internos sensibles, como Jira.
- Implementar monitoreo continuo en plataformas críticas para detectar actividades inusuales o no autorizadas.
- Establecer un plan de respuesta ante incidentes con simulaciones periódicas para preparar a los equipos frente a ataques similares.
- Realizar auditorías regulares en sistemas internos para identificar vulnerabilidades potenciales y corregirlas de manera proactiva.

5. REFERENCIAS:

- https://www.securityweek.com/schneider-electric-launches-probe-after-hackers-claim-theft-of-user-data/

Seguridad ICS: 145.000 sistemas expuestos a la Web, numerosas empresas industriales afectadas por ataques

Tipo de Ataque: Exposición de sistemas ICS a Internet

Medio de Propagación: Accesibilidad directa a través de protocolos comunes de comunicación industrial

1. PRODUCTOS AFECTADOS:

- Sistemas accesibles mediante:
- Modbus, Fox, BACnet, WDBRPC (Wind River)
- EIP, S7 (Siemens), IEC 60870-5-104
- Interfaces Hombre-Máquina (HMI): 34% vinculadas a sistemas de agua, 23% al sector agrícola.

2. RESUMEN:

Un informe de Censys revela que más de 145000 sistemas de control industrial (ICS) están expuestos a internet en 175 países. Estados Unidos lidera con 48000 sistemas detectados. Estos dispositivos utilizan protocolos comunes que facilitan su explotación por actores maliciosos, destacando la vulnerabilidad de sectores como el agua y la agricultura. Además, una encuesta de Kaspersky indica que el 90% de las empresas industriales del Reino Unido han sido víctimas de ciberataques, y el 72% perciben que sus cadenas de suministro automatizadas son vulnerables.

3. DETALLE:

El informe de Censys destaca que las regiones presentan diferencias significativas en el uso de protocolos industriales. En América del Norte predominan protocolos como Fox, BACnet, ATG y C-More, mientras que en Europa se utilizan más Modbus, S7, e IEC 60870-5-104. Muchas de las instancias expuestas corresponden a interfaces Hombre-Máquina (HMI), de las cuales el 34% están vinculadas a sistemas de agua y el 23% al sector agrícola, sectores especialmente vulnerables a ataques. Además, se detectaron casi 200 hosts que combinan HMI con productos prohibidos bajo la Sección 889 de la Ley de Autorización de Defensa Nacional (NDAA) de Estados Unidos. Esto subraya la importancia de evaluar cuidadosamente el software y los productos utilizados en procesos industriales para mitigar riesgos asociados a la exposición de estos sistemas.

4. RECOMENDACIONES:

- Aislar los sistemas ICS de redes accesibles desde Internet mediante una segmentación adecuada para reducir su exposición.
- Implementar autenticación robusta y restringir el acceso a las interfaces HMI únicamente al personal autorizado.
- Utilizar herramientas de monitoreo continuo, como SIEM, para identificar actividades inusuales o potencialmente maliciosas.
- Realizar evaluaciones periódicas de seguridad en protocolos y dispositivos para identificar y corregir vulnerabilidades de manera positiva.
- Capacitar a los operadores y administradores en las mejores prácticas de ciberseguridad, priorizando la protección de sistemas críticos.

5. REFERENCIAS:

- https://www.securityweek.com/american-water-cyberattack-renews-focus-on-protecting-critical-infrastructure/