Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Octubre - 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:

- EE.UU. afirma que hackers chinos atacaron a varios proveedores de telecomunicaciones
- El ransomware Black Basta se hace pasar por soporte de TI en Microsoft Teams para vulnerar las redes.
- Reportan venta de información sensible de 140 empresas peruanas en la Dark Web

Alertas de Seguridad OT/ICS:

- Las organizaciones detectan más rápidamente los incidentes de OT, pero la respuesta sigue siendo deficiente, según un informe
- SIGA lanza una suite de detección y respuesta a amenazas OT
- El ciberataque a American Water renueva el foco en la protección de infraestructuras críticas

EE. UU. afirma que hackers informáticos chinos atacaron a varios proveedores de telecomunicaciones

Tipo de Ataque: Espionaje Cibernético

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Servicios de Telecomunicaciones

2. **RESUMEN:**

La agencia federal Centros de Servicios de Medicare y Medicaid (CMS) ha informado que más de tres millones de beneficiarios de planes de salud vieron expuesta su información personal y de salud debido a los ataques MOVEit del ransomware Cl0p. Estos datos fueron robados tras una violación en la seguridad de Wisconsin Physicians Service (WPS), una empresa que administra servicios de Medicare.

3. **DETALLE:**

El ciberataque afectó a CMS, una agencia que administra los programas de atención médica más grandes de Estados Unidos, como Medicare, Medicaid y CHIP. CMS reportó el incidente a través de un comunicado de prensa el 6 de septiembre, donde notificó que 946,801 personas con Medicare fueron afectadas directamente. No obstante, el número total de personas afectadas asciende a 3.112.815, según el portal de violaciones de datos del Departamento de Salud y Servicios Humanos de EEUU (HHS).

El ataque se produjo mediante una vulnerabilidad en MOVEit Transfer, un software utilizado por WPS para gestionar datos. Aunque WPS aplicó los parches de seguridad en junio de 2023, una revisión realizada en mayo de 2024 reveló que los piratas informáticos habían accedido a la red antes de que se implementaran dichas actualizaciones, lo que permitió la exfiltración de archivos sensibles.

CMS ha tomado medidas inmediatas para notificar a los afectados y coordinar con WPS, que ha iniciado un proceso de investigación y refuerzo de seguridad. El ataque Cl0p pone de relieve la vulnerabilidad de los sistemas de gestión de datos y la importancia de implementar actualizaciones de seguridad de manera proactiva y oportuna.

4. **RECOMENDACIONES:**
   - Realizar auditorías de seguridad exhaustivas en los sistemas de telecomunicaciones y comunicaciones críticas.
   - Implementar autenticación multifactor, monitoreo de tráfico de red y capacitación contra ataques de phishing.
   - Reforzar las defensas cibernéticas en colaboración con agencias gubernamentales para proteger la infraestructura de telecomunicaciones ante amenazas de ciberespionaje

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/us-says-chinese-hackers-breached-multiple-telecom-providers/

El ransomware Black Basta se hace pasar por soporte de TI en Microsoft Teams para vulnerar las redes.

Tipo de Ataque: Ingeniería Social y Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Microsoft Teams
2. **RESUMEN:**

La operación de ransomware Black Basta ha evolucionado en sus tácticas de ataque mediante el uso de Microsoft Teams para llevar a cabo ataques de ingeniería social. Ahora, los actores maliciosos contactan a empleados de empresas haciéndose pasar por soporte técnico a través de Teams, simulando asistencia para resolver un problema de spam. Su objetivo es obtener acceso remoto a los dispositivos de las víctimas e instalar herramientas de control, lo que les permite propagar el ransomware y comprometer la red corporativa.

3. **DETALLE**

Black Basta es un grupo de ransomware activo desde 2022, que ha afectado a numerosas empresas mediante técnicas de ingeniería social y vulnerabilidades en redes. En esta nueva táctica, el ataque inicia con el envío masivo de correos electrónicos no maliciosos que saturan la bandeja de entrada de los empleados. Los atacantes luego los contactan a través de Microsoft Teams, desde cuentas de apariencia legítima, haciéndose pasar por el equipo de soporte de TI. Utilizando perfiles como "Help Desk" o "Security Admin", engañan a los empleados para que instalen herramientas de acceso remoto, como AnyDesk o Quick Assist.

Una vez que los actores maliciosos logran acceso al dispositivo de la víctima, instalan diversas cargas útiles, como "AntispamAccount.exe" y Cobalt Strike, que facilitan un acceso continuo a la red y permiten la implementación del ransomware. ReliaQuest ha observado también el uso de cuentas falsas de soporte técnico y enlaces de códigos QR, posiblemente para guiar a las víctimas a sitios maliciosos.

4. **RECOMENDACIONES:**
   - Restringir las comunicaciones de usuarios externos en Microsoft Teams, permitiendo solo aquellos provenientes de dominios confiables.
   - Implementar registros de eventos en Teams, particularmente el evento “ChatCreated”, para detectar chats sospechosos.
   - Capacitar a los empleados en la identificación de ataques de ingeniería social y phishing, y enfatizar la verificación de contactos de soporte técnico.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/black-basta-ransomware-poses-as-it-support-on-microsoft-teams-to-breach-networks/

Reportan venta de información sensible de 140 empresas peruanas en la Dark Web

Tipo de Ataque: **Exposición de Datos en la Dark Web**

Medio de Propagación: **Internet**

1. **PRODUCTOS AFECTADOS:**
   - 140 empresas peruanas de diferentes sectores
   - Información sensible de varias industrias expuestas
2. **RESUMEN**

Según un estudio de la Cámara de Comercio de Lima, se proyecta que para 2028 las empresas peruanas invertirán hasta $500 millones en seguridad digital. Sin embargo, redes clandestinas como la Dark Web ya están generando problemas significativos, donde datos filtrados de empresas peruanas están a la venta. Soluciones Virtuales Perú identificó incidentes verificados en 140 empresas, lo cual plantea serios riesgos de seguridad y reputación.

3. **DETALLE:**

El estudio "Análisis Profundo No Invasivo de Exposición de Datos y Monitorización de la Dark Web" reveló que una variedad de datos robados, desde credenciales de acceso hasta información financiera, están circulando activamente en la Dark Web. Sectores como finanzas, salud y retail han sido especialmente afectados. La exposición de estos datos no solo compromete a las empresas, sino también a sus clientes y empleados, dado el riesgo de fraudes, robo de identidad y otros ataques.

4. **RECOMENDACIONES**
   - Implementar herramientas de monitoreo de la Dark Web para detectar posibles filtraciones de datos en tiempo real.
   - Fortalecer las políticas de ciberseguridad y formación en gestión de datos sensibles.
   - Establecer procesos de respuesta a incidentes que incluyan la evaluación continua de vulnerabilidades y simulacros de contingencia.

5. **REFERENCIAS:**
   - https://gestion.pe/economia/empresas/reportan-venta-de-informacion-sensible-de-140-empresas-peruanas-en-la-dark-web-ciberseguridad-ataques-ciberneticos-deep-web-banca-estafa-tecnologia-noticia/?ref=gesr

Las organizaciones detectan más rápidamente los incidentes de OT, pero la respuesta sigue siendo deficiente

1. PRODUCTOS AFECTADOS:

- Infraestructura de Tecnología Operativa (OT)
- Sistemas de control industrial (ICS)

2. RESUMEN:

Un informe reciente del SANS Institute titulado State of ICS/OT Cybersecurity 2024 revela que, aunque las organizaciones han mejorado en la detección de incidentes en sistemas de control industrial (ICS) y entornos OT, la respuesta a estos sigue siendo insuficiente. La encuesta, que incluyó a más de 530 profesionales de infraestructura crítica, muestra que el 60% de los encuestados puede detectar un ataque en menos de 24 horas, una mejora en comparación con hace cinco años. Sin embargo, solo el 56% de las organizaciones cuenta con un plan específico de respuesta a incidentes para ICS/OT.

3. DETALLE:

Según el informe de SANS, los ataques de ransomware han disminuido, afectando solo al 12% de las organizaciones OT en los últimos 12 meses, aunque otros incidentes siguen siendo comunes. Aproximadamente el 38% de los ataques impactaron la seguridad y confiabilidad de los procesos físicos, y en un 46% de los casos el ataque inicial involucró una vulneración de TI que dio acceso a sistemas OT. Las vías de ataque iniciales incluyeron servicios remotos externos, dispositivos expuestos a Internet, estaciones de trabajo de ingeniería, unidades USB comprometidas, spearphishing, y ataques a la cadena de suministro.

Las organizaciones que realizan pruebas de sus planes de respuesta a incidentes trimestral o mensualmente muestran una mayor confianza en su capacidad de operar los ICS en modo manual. El informe sugiere que pruebas más frecuentes, que integran inteligencia de amenazas y escenarios impulsados por consecuencias, fortalecen la respuesta ante incidentes en OT.

4. RECOMENDACIONES:

- Desarrollar y probar regularmente un plan específico de respuesta a incidentes para ICS/OT, idealmente al menos cada trimestre.
- Incrementar la protección de dispositivos expuestos a Internet y reforzar los controles en servicios remotos externos para reducir los vectores de ataque.
- Integrar inteligencia de amenazas en las evaluaciones de seguridad para mejorar la capacidad de respuesta en ICS/OT y prevenir el acceso no autorizado a los sistemas críticos.

5. REFERENCIAS:

- https://www.securityweek.com/organizations-faster-at-detecting-ot-incidents-but-response-still-lacking-report/

SIGA lanza una suite de detección y respuesta a amenazas OT

1. **PRODUCTOS AFECTADOS:**
   - Infraestructura de Tecnología Operativa (OT)
   - Redes industriales y sistemas de control

2. **RESUMEN:**

En la Conferencia de Ciberseguridad ICS SecurityWeek 2024 en Atlanta, SIGA, una empresa de seguridad en OT ha presentado su nueva suite de ciberseguridad OT llamada SIGA SigaML 2. Esta solución está diseñada para proteger infraestructuras industriales mediante un enfoque de aprendizaje automático de múltiples capas que permite a los CISO detectar amenazas, responder a incidentes y mejorar la capacitación de sus equipos de ciberseguridad. Uno de los componentes clave de la suite, SigaGuardX, utiliza inteligencia artificial y datos de diversas fuentes para identificar posibles ataques cibernéticos en OT que podrían pasar desapercibidos en otros sistemas.

3. **DETALLE:**

En el pasado, los sistemas de agua y aguas residuales han sido blanco de ataques cibernéticos, incluidos ransomware y otros incidentes que comprometieron su operación. Estos eventos resaltan la necesidad de mayor inversión en ciberseguridad para proteger este sector crítico. La nueva suite SigaML 2 de SIGA incluye tecnologías avanzadas de IA y aprendizaje automático para proteger redes de OT. Uno de sus componentes principales, SigaGuard, ofrece visibilidad a nivel 0 (zona de proceso físico) mediante sensores de hardware, permitiendo identificar posibles ataques a nivel de procesos. Además, SigaGuardX incorpora la herramienta S-PAS, diseñada para entrenar a los equipos de operaciones y ciberseguridad a través de simulaciones de escenarios de ataque, mejorando así la preparación ante posibles incidentes.

El director ejecutivo de SIGA, Amir Samoiloff, destacó que los ciberataques en OT son cada vez más sofisticados y que la nueva suite SigaML 2 proporciona a los CISO herramientas clave para detectar amenazas y gestionar ataques con el apoyo de un sistema de soporte de decisiones OT (OT_DSS). La solución también incluye un simulador de ataques integrado, que ayuda a los equipos a prepararse y responder adecuadamente ante diversos escenarios.

4. **RECOMENDACIONES:**
   - Implementar herramientas de visibilidad de nivel 0, como sensores de hardware, para identificar amenazas en los procesos físicos de OT.
   - Utilizar sistemas de simulación de ataques y escenarios de ciberseguridad para mejorar la capacitación y preparación de los equipos de operaciones y ciberseguridad.
   - Integrar soluciones de IA/ML en las infraestructuras OT para detectar anomalías y responder a incidentes de forma oportuna, minimizando el impacto de posibles ciberataques

5. **REFERENCIAS:**

- https://www.securityweek.com/siga-launches-ot-cybersecurity-suite-for-cisos/

El ciberataque a American Water renueva el foco en la protección de infraestructuras críticas

Tipo de Ataque: Acceso No Autorizado

Medio de Propagación: Sistemas TI

1. **PRODUCTOS AFECTADOS:**
   - Infraestructura de Tecnología Operativa (OT)
   - Redes industriales y sistemas de control

2. **RESUMEN:**

American Water, la mayor empresa regulada de servicios de agua y aguas residuales en Estados Unidos ha sufrido un ciberataque que ha afectado sus sistemas de facturación, renovando la atención sobre la protección de infraestructuras críticas. La empresa, que atiende a más de 14 millones de personas en 14 estados y 18 instalaciones militares, detectó la actividad no autorizada y respondió de inmediato cerrando ciertos sistemas. Sin embargo, los servicios de agua y alcantarillado no se han visto afectados, y el personal continúa trabajando para investigar el alcance del ataque.

3. **DETALLE:**

El ciberataque en American Water, con sede en Nueva Jersey, fue detectado el jueves y ha llevado a la suspensión temporal de la facturación a clientes como medida de precaución. Aunque el ataque no parece haber comprometido la operación de los sistemas de agua, la situación destaca la vulnerabilidad de infraestructuras críticas ante amenazas cibernéticas. Según Jack Danahy, vicepresidente de NuHarbor Security, el ataque se centró en los sistemas de TI y no en la parte operativa. La creciente digitalización de servicios de facturación y atención al cliente incrementa los riesgos de seguridad en estos sectores.

La Agencia de Seguridad Cibernética e Infraestructura (CISA) y la Agencia de Protección Ambiental (EPA) han advertido que el 70% de los servicios públicos inspeccionados no cumplen completamente con las normas de seguridad, lo que eleva el riesgo de futuros ataques. Ambas agencias instan a las empresas del sector a reforzar sus medidas de protección para proteger el suministro de agua potable del país.

4. **RECOMENDACIONES:**
   - Realizar auditorías regulares de seguridad en los sistemas de TI y mejorar la detección de amenazas para evitar accesos no autorizados.
   - Implementar un sistema de respuesta rápida ante incidentes, con protocolos definidos para minimizar el impacto en caso de ataques.
   - Colaborar con agencias de ciberseguridad nacionales para evaluar y mejorar las protecciones en infraestructuras críticas, especialmente en sectores que afectan el suministro de agua y otros servicios esenciales.

5. **REFERENCIAS:**

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