Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Agosto - 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 agosto.

Alertas de Seguridad IT:

- Patelco notifica a 726.000 clientes sobre una violación de datos de Ransomware
- AMD sufre segundo ciberataque en 2024: datos confidenciales a la venta en la Dark Web
- India enfrenta un aumento alarmante de ciberataques contra su infraestructura crítica

Alertas de Seguridad OT/ICS:

- Gigante petrolero Halliburton sufre ciberataque que paraliza sus sistemas
- ISAGCA publica guía sobre implementación de Zero Trust en sistemas de control industrial

Patelco notifica a 726.000 clientes sobre una violación de datos de ransomware

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Red
2. **RESUMEN:**

Patelco Credit Union, una cooperativa de ahorro y crédito estadounidense sin fines de lucro advierte a 726,000 clientes que ha sido víctima de un ataque de Ransomware RansomHub. Este incidente interrumpió varias operaciones internas, aunque los servicios de los clientes no se vieron afectados de inmediato. Las autoridades confirmaron que los datos confidenciales de los usuarios y las operaciones internas se encontraban en riesgo, pero lograron detener la amenaza antes de que se propagara por completo. En la actualidad, la institución está tomando las medidas necesarias para mitigar el impacto y mejorar la seguridad de sus sistemas

3. **DETALLE:**

En agosto del 2024, Patelco Credit Union una de las principales cooperativas en Estados Unidos, sufrió un ciberataque por medio de una infiltración de Ransomware en su red interna.

Los atacantes lograron explotar una vulnerabilidad en los sistemas de la organización, lo que permitió desplegar el ransomware sin ser detectados inicialmente. A medida que los sistemas empezaron a fallar, la institución tomó medidas para contener el daño y evitar la propagación del malware a otros sistemas conectados.

El ataque permitió a los ciberdelincuentes acceder a información sensible, incluyendo datos personales y financieros de aproximadamente 726,000 clientes. Aunque los sistemas de atención al cliente permanecieron operativos, la organización trabajó junto al FBI para investigar el incidente y poder mitigar sus efectos.

Patelco decidió informar de manera proactiva a todos los clientes sobre la violación de datos. La institución ofreció servicios de monitoreo de crédito y protección contra el robo de identidad a los clientes afectados, minimizando posibles daños adicionales derivados del incidente.

Finalmente, Patelco se encuentra reforzando sus medidas de ciberseguridad con el objetivo de prevenir futuros ataques y están trabajando con expertos en ciberseguridad para identificar cualquier otra posible vulnerabilidad en sus sistemas, asegurando la protección de datos de sus miembros.

4. RECOMENDACIONES:

- Concientizar al personal para que evite los correos de phishing o con malware, las memorias USB infectadas, el software pirata u otros canales de infección.
- Mantener actualizado un buen EDR/antimalware en todos los equipos.
- Escanear periódicamente la red interna y las IPs públicas para detectar vulnerabilidades y establecer planes de remediación.
- Implementar un plan de respuesta y recuperación ante incidentes, que incluya un programa de backups y de pruebas de restauración.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/patelco-notifies-726-000-customers-of-ransomware-data-breach/

AMD sufre segundo ciberataque en 2024: datos confidenciales a la venta en la dark web

Tipo de Ataque: Brecha de datos

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   Repositorio de datos
2. **RESUMEN:**

Advanced Micro Devices (AMD), una de las principales empresas de semiconductores, fue víctima de un segundo ciberataque significativo en 2024. Este incidente, atribuido a los grupos criminales IntelBroker y EnergyWeaponUser, resultó en el robo de datos sensibles que ahora se ofrecen a la venta en mercados de la dark web, subrayando la creciente vulnerabilidad de las empresas tecnológicas frente a las amenazas cibernéticas.

3. **DETALLE**

El 28 de agosto de 2024, se reveló que AMD había sufrido un nuevo ciberataque, apenas dos meses después de un incidente similar ocurrido en junio del mismo año. En esta ocasión, los atacantes lograron acceder y robar diversos tipos de información confidencial, incluyendo credenciales de usuario, resoluciones internas y descripciones detalladas de casos.

Los grupos criminales responsables, IntelBroker y EnergyWeaponUser, pusieron a la venta la información robada en BreachForums, un conocido mercado de la dark web. Este hecho marcó la segunda vez en el año que las comunicaciones internas y la información sensible de los empleados de AMD se vieron comprometidas por ciberataques.

IntelBroker, uno de los grupos implicados en el ataque, había sido previamente vinculado a supuestas brechas en otras organizaciones de alto perfil, como Europol y T-Mobile, aunque ambas entidades negaron haber sufrido compromisos en sus sistemas. La reiteración de estos ataques evidenció la persistencia y sofisticación de los grupos cibercriminales.

En respuesta al incidente, AMD reconoció las afirmaciones sobre el ataque, pero no proporcionó una verificación detallada ni un comentario exhaustivo sobre lo ocurrido. La empresa informó que estaba colaborando con las fuerzas del orden y un socio de alojamiento externo para investigar la situación y evaluar el alcance de la filtración de datos.

Este ataque a AMD, una empresa líder en la fabricación de chips para IA, subrayó las preocupaciones sobre las amenazas continuas que enfrentan las compañías tecnológicas de vanguardia. La serie de ciberataques recientes sirvió como un recordatorio alarmante de los peligros omnipresentes en el panorama digital actual.

4. **RECOMENDACIONES:**
   - Gestionar el nivel de ciberseguridad de los proveedores que mantienen o acceden a nuestra información sensible.

- Asegurar que todo acceso a información en la nube, desde fuera de las oficinas, use autenticación de múltiples factores (MFA).
- Evaluar si puede haber información de los stakeholders de su organización en la brecha publicada y posibles medidas a tomar en caso de que sea así.

5. REFERENCIAS:

- https://www.newsbytesapp.com/news/science/amd-suffers-second-major-cyberattack-this-year/story

India enfrenta un aumento alarmante de ciberataques contra su infraestructura crítica

Tipo de Ataque: Ataque

Medio de Propagación: Internet

1. RESUMEN:

Los sectores financiero y gubernamental de India experimentaron un incremento significativo en ciberataques, llevando al Banco de Reserva de India (RBI) a instar a las entidades bancarias a reforzar sus medidas de ciberseguridad. Este aumento en las amenazas cibernéticas puso de manifiesto la vulnerabilidad de las infraestructuras críticas del país en plena era de digitalización.

2. DETALLE:

La rápida digitalización de diversos sectores de infraestructura crítica en India, desde finanzas hasta sistemas gubernamentales, y desde manufactura hasta salud, los convirtió en blancos atractivos para ciberataques. En abril de 2024, un grupo de hackers filtró 7,5 millones de registros con información personal robada de boat, el principal fabricante indio de dispositivos de audio inalámbricos y wearables.

El Banco de Reserva de India (RBI) advirtió sobre los riesgos potenciales que la creciente digitalización representaba para la infraestructura financiera del país. Según un informe del RBI, los incidentes cibernéticos en el sector financiero, manejados por el equipo nacional CERT, se dispararon de 53.000 en 2017 a 16 millones en 2023.

La mayoría de los bancos y las compañías financieras no bancarias (NBFCs) consideraron la ciberseguridad como el principal desafío para su transición a tecnologías digitales. El RBI señaló que la digitalización podría plantear preocupaciones para la estabilidad financiera debido a las amenazas de ciberseguridad, las violaciones de datos y la rapidez con la que la información y los rumores podían propagarse por el sistema.

El sector público y los sistemas gubernamentales también experimentaron un aumento dramático en los ciberataques, con la mayoría de las instalaciones registrando un crecimiento de al menos el 50% en incidentes. A principios de 2024, un grupo de hackers dirigió sus ataques contra agencias gubernamentales y empresas energéticas utilizando un troyano denominado HackBrowserData.

India se posicionó como el cuarto país más afectado en la región Asia-Pacífico, con el 83% de las organizaciones reportando al menos un incidente de ciberseguridad en el último año, según un informe de Cloudflare. A nivel global, el país ocupó el quinto lugar en términos de violaciones de seguridad.

Las principales preocupaciones de las organizaciones indias incluyeron amenazas relacionadas con la nube (52%), ataques a dispositivos conectados (45%), operaciones de hackeo y filtración (36%), y compromisos en la cadena de suministro de software (35%). La adopción de tecnologías emergentes como IA y nube, junto con el enfoque en innovación y trabajo remoto, impulsó las transformaciones digitales, aumentando la necesidad de mayores defensas de seguridad.

El crecimiento de la IA también moldeó el panorama de amenazas en el país, con actores maliciosos experimentando con diferentes modelos y técnicas de IA. Se esperaba que los atacantes utilizaran IA para

generar malware personalizado y polimórfico basado en exploits de sistemas, evadiendo los métodos de detección tradicionales y basados en firmas.

3. RECOMENDACIONES

- Realizar una evaluación de postura de seguridad, para establecer un roadmap de mejora a nivel estratégico táctico.
- Implementar un Sistema de Gestión de Seguridad de Información (SGSI) que permita una mejora continua de la ciberseguridad.

4. REFERENCIAS:

- https://www.darkreading.com/cyber-risk/india-s-critical-infrastructure-suffers-spike-in-cyberattacks

Gigante petrolero Halliburton sufre ciberataque que paraliza sus sistemas

Tipo de Ataque: Desconocido

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Dispositivo ICS
2. **RESUMEN:**

Halliburton, una de las mayores empresas de servicios energéticos del mundo, ha confirmado ser víctima de un ciberataque que la obligó a desconectar parte de sus sistemas. Este incidente resalta la vulnerabilidad de las infraestructuras críticas y la importancia de la ciberseguridad en el sector energético.

3. **DETALLE:**

Halliburton, fundada en 1919 y con más de 40,000 empleados en todo el mundo, se enfrenta a un desafío significativo tras el reciente ciberataque. La empresa, que reportó ingresos de $5.8 mil millones y un margen operativo del 18% para el segundo trimestre de 2024, podría ver afectadas sus operaciones globales debido a este incidente.

En respuesta al ataque, la compañía ha implementado una serie de medidas de contingencia. Además de la desconexión de sistemas críticos, Halliburton ha iniciado una investigación interna respaldada por asesores externos especializados en ciberseguridad. Esta acción demuestra la seriedad con la que la empresa está abordando la situación y su compromiso con la protección de datos e infraestructuras críticas.

Un aspecto crucial de la respuesta de Halliburton ha sido su comunicación transparente. La empresa no solo ha notificado a las autoridades pertinentes, incluyendo agencias de aplicación de la ley, sino que también ha presentado un informe oficial ante la Comisión de Bolsa y Valores de Estados Unidos (SEC). Este nivel de transparencia es fundamental en un sector tan regulado y sensible como el energético.

El Sistema de Gestión Halliburton, un marco integral de seguridad y operaciones, está siendo puesto a prueba durante esta crisis. La empresa ha asegurado que continúa operando bajo sus estándares de seguridad basados en procesos, lo que podría ser clave para minimizar el impacto del ataque en sus operaciones diarias y en la prestación de servicios a sus clientes globales.

La naturaleza exacta del ataque sigue siendo un misterio. Un portavoz del Departamento de Energía de EE.UU. confirmó que se desconocen los detalles específicos del incidente, lo que ha generado especulaciones sobre su alcance y posibles motivaciones. Esta incertidumbre subraya la complejidad de los ciberataques modernos y los desafíos que enfrentan incluso las empresas más grandes y sofisticadas en términos de ciberseguridad.

El incidente de Halliburton se produce en un contexto de creciente preocupación por la seguridad de las infraestructuras críticas. Recuerda al ataque de ransomware contra Colonial Pipeline en 2021, que causó interrupciones significativas en el suministro de combustible en la costa este de Estados Unidos.

4. RECOMENDACIONES:

- Realizar una evaluación de postura de seguridad, para establecer un roadmap de mejora a nivel estratégico táctico.
- Implementar un Sistema de Gestión de Seguridad de Información (SGSI) que permita una mejora continua de la ciberseguridad.

5. REFERENCIAS:

- https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/la-petrolera-halliburton-sufre-un-ciberataque

ISAGCA publica guía sobre implementación de Zero Trust en sistemas de control industrial

1. RESUMEN:

La Alianza Global de Ciberseguridad ISA (ISAGCA) lanzó un documento técnico que analiza la aplicación del modelo de seguridad Zero Trust en tecnologías operativas (OT) y sistemas de control industrial (ICS). El informe proporciona orientación sobre cómo implementar principios de Zero Trust utilizando los estándares ISA/IEC 62443, destacando la importancia de priorizar la seguridad en entornos OT.

2. DETALLE:

El 14 de agosto de 2024, la ISAGCA publicó un documento técnico titulado "Resultados de Zero Trust utilizando los estándares ISA/IEC 62443". Este informe examinó la aplicación del modelo de ciberseguridad Zero Trust en el contexto de tecnologías operativas (OT) y sistemas de control industrial (ICS).

El modelo Zero Trust se ha convertido en una estrategia de ciberseguridad ampliamente aceptada, basada en la premisa de que el riesgo es inherente tanto interna como externamente. Este enfoque ha ganado relevancia en entornos OT, donde se pueden incorporar principios de Zero Trust mediante enfoques híbridos cuando sea apropiado.

El documento de ISAGCA analizó el uso de la serie de estándares ISA/IEC 62443 para implementar Zero Trust en OT. Estos estándares son reconocidos mundialmente como la principal referencia basada en consenso para la ciberseguridad de sistemas de control.

Una recomendación clave del informe fue que el modelo Zero Trust no debería introducirse para funciones esenciales según lo definido en ISA/IEC 62443. El documento enfatizó la importancia de nunca anular o interrumpir funciones críticas esenciales en implementaciones de arquitectura Zero Trust, especialmente las funciones de seguridad asociadas con el diseño de sistemas tolerantes a fallos.

El informe reconoció que la implementación de Zero Trust podría implicar costos adicionales iniciales y de mantenimiento, ya que eleva las dimensiones y la magnitud de la seguridad. Sin embargo, también ofreció beneficios significativos en términos de comprensión y organización de una estrategia de seguridad.

ISAGCA señaló que, si ciertos principios de Zero Trust no son factibles de implementar dentro de una red OT, se pueden incorporar enfoques híbridos donde sea apropiado. Esto permitiría mejorar las capacidades de detección y respuesta a escala, manteniendo la integridad y seguridad de los sistemas críticos.

El documento proporcionó una guía valiosa para profesionales de seguridad y gerentes de sistemas industriales, ayudándoles a navegar la compleja intersección entre las mejores prácticas de ciberseguridad modernas y los requisitos únicos de los entornos OT e ICS.

3. RECOMENDACIONES:

- Revisar la documentación y establecer la aplicabilidad en el contexto de su organización.
- Recurrir a apoyo experto para establecer planes concretos adaptados a su organización

4. REFERENCIAS:

- https://www.automation.com/en-us/articles/august-2024/isagca-report-zero-trust-outcomes-ot-cybersecurity?listname=Articles%20&%20News%20on%20Cybersecurity