Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín Informativo

Veinte

Febrero: Tendencias de amenazas de ciberseguridad previstas para el año 2030

Documento recuperado de ENISA

VIEM Vicerrectoría de Innovación y Emprendimiento

ECBTI Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación Ceros y Unos

SIELSIC

Invitado Especial: ESCUELA DE COMUNICACIONES MILITARES
CENTRO DE INVESTIGACIÓN (CEINV)

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veinte
Febrero de 2024

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director
CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
SV. Correa Cobos Jennifer- **ESCOM**
Ing. Yeison Alfonso Buitrago Rojas - **ESCOM**

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 20

Febrero 2024

Tendencias de amenazas de ciberseguridad previstas para el año 2030

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

"ENISA (Agencia de la Unión Europea para la Ciberseguridad) es la agencia de la Unión Europea a la que se le ha encomendado la misión de velar por un alto nivel común de ciberseguridad en toda Europa"[1]

En su publicación titulada de fecha 13 de septiembre de 2023: "Foresight 2030 Threats", presenta los próximos retos para la disciplina de la Ciberseguridad, donde Juhan Lepassaar Director Ejecutivo de ENISA indica que "*el panorama de amenazas cibernéticas es un ecosistema complejo de amenazas, actores y técnicas de ataque que también están sujetas a la influencia de eventos mundiales como pandemias y geopolítica. Aunque no podemos predecir el futuro, tenemos el deber de anticipar las tendencias emergentes y los patrones. En 2021*[2]*, ENISA desarrolló un marco metodológico de previsión de ciberseguridad basado en la investigación prospectiva y los estudios futuros. Este marco se utilizó por primera vez en 2022 para diseñar escenarios futuros e identificar amenazas y desafíos que probablemente surgirán para 2030*".

Aunque ENISA pone como año visionado el 2030, en la actualidad ya algunas de estas amenazas han sido evidenciadas.

[1] https://www.enisa.europa.eu/about-enisa/about/es
[2] https://www.enisa.europa.eu/publications/foresight-challenges

Desarrollo

Campañas de desinformación avanzadas

La utilización de técnicas sofisticadas para difundir información falsa y engañosa, tienen como propósito manipular comunidades y lograr objetivos políticos o económicos. Estas campañas pueden incluir el uso de deepfakes, que son videos o imágenes manipuladas las cuales parecen auténticas, pero en realidad son falsas. Así mismo, estas campañas pueden tener un impacto significativo en la opinión pública, la toma de decisiones y la estabilidad social.

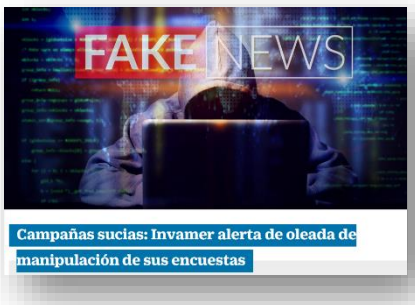

Imagen 1: Recuperado de https://www.eltiempo.com

Este tema no es ajeno para Colombia, en las últimas elecciones se publicaron numerosas noticias falsas. Estas podrían haber sido parte de estrategias de desinformación avanzada, con el objetivo de manipular comunidades por razones geopolíticas o para obtener beneficios económicos. Ver artículo de periódico el tiempo titulado: "Campañas sucias: Invamer alerta de oleada de manipulación de sus encuestas"

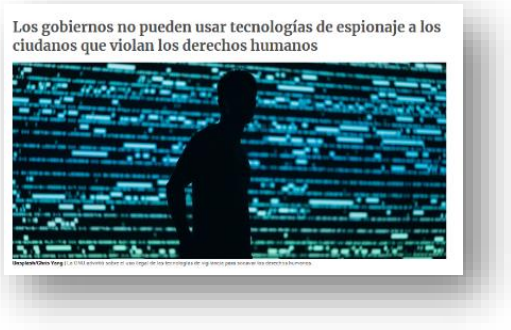

Imagen 2: Recuperado de: https://news.un.org/es/story/2021/07/1494542

Auge del autoritarismo de vigilancia digital / pérdida de privacidad

El aumento de la vigilancia digital por parte de regímenes autoritarios impacta en una pérdida de privacidad y posibles abusos contra los derechos humanos. Los actores potenciales de esta amenaza incluyen grupos patrocinados por el estado y organizaciones criminales. Estos utilizan técnicas de ataque como la de hombre en el medio, software malicioso, el uso de certificados falsos y el abuso de datos personales para llevar a cabo la vigilancia y afectar la privacidad de las personas. Los impactos potenciales incluyen violaciones de privacidad y abusos contra los derechos humanos.

*"La Alta Comisionada de la ONU para los Derechos Humanos consideró "**extremadamente alarmantes"** las informaciones que dan cuenta de un uso generalizado en distintos países del software Pegasus para espiar a periodistas, defensores de los derechos humanos, políticos y otras personalidades públicas"*[3]

[3] https://news.un.org/es/story/2021/07/1494542

Error humano y sistemas heredados explotados dentro de los ecosistemas ciberfísicos

Hace referencia a la posibilidad que los errores humanos y las vulnerabilidades en los sistemas heredados dentro de los entornos ciberfísicos puedan ser aprovechados por ciberdelincuentes. Los sistemas heredados por lo general carecen de las medidas de seguridad y actualizaciones necesarias, lo que los hace vulnerables a ciberataques. Además, los errores humanos, como la falta de capacitación o el descuido, pueden abrir brechas de seguridad en estos sistemas. Por ejemplo, un atacante podría aprovechar una vulnerabilidad en un sistema heredado utilizado en una planta industrial para acceder y manipular los procesos de producción, causando daños o interrupciones significativas.

Ataques dirigidos mejorados por datos de dispositivos inteligentes (Ransomware como ejemplo)

Hace referencia a la utilización de datos obtenidos de dispositivos inteligentes conectados a Internet para llevar a cabo ataques más sofisticados y personalizados. Los adversarios o ciberdelincuentes pueden acceder a información a través de estos dispositivos para obtener detalles específicos sobre sus víctimas y utilizarlos en ataques dirigidos. Por ejemplo, los ciberdelincuentes pueden utilizar datos recopilados de dispositivos inteligentes en el hogar, como cámaras de seguridad o sistemas de temperatura inteligentes, para obtener información sobre los patrones de vida de una persona y utilizarla en un ataque de ransomware personalizado. Esto les permite cifrar los archivos y sistemas de la víctima de manera más efectiva, aumentando las posibilidades que paguen el rescate.

Falta de análisis y control de la infraestructura y objetos basados en el espacio

Hace referencia a la falta de comprensión, análisis y control de la seguridad de la infraestructura y los objetos basados en el espacio. Esto puede hacer que estos sistemas sean vulnerables al inicio de ataques e interrupciones. La falta de comprensión de la seguridad de la infraestructura espacial puede permitir que actores malintencionados realicen ataques y provoquen fallas en los sistemas. Por ejemplo, un atacante podría comprometer la infraestructura espacial para sabotear operaciones comerciales o gubernamentales durante conflictos geopolíticos.

Auge de amenazas híbridas avanzadas

Hace referencia al aumento de las amenazas que combinan diferentes elementos y tácticas, como ciberataques, guerra cibernética, guerra convencional, desinformación y manipulación de la opinión pública. Estas amenazas híbridas avanzadas pueden ser llevadas a cabo por grupos criminales u otros actores malintencionados. Utilizan una combinación de métodos y herramientas para lograr sus objetivos, como el uso de ataques cibernéticos para desestabilizar infraestructuras críticas, la propagación de desinformación para socavar la confianza en las instituciones y la manipulación de los ciudadanos a través de las redes sociales. Estas amenazas híbridas avanzadas representan un desafío significativo para la seguridad nacional y requieren de una respuesta integral y coordinada.

Escasez de habilidades

Hace referencia a la falta de personal entrenado y competente en el campo de la ciberseguridad. Esta escasez de habilidades puede llevar a una brecha en la capacidad de las organizaciones para protegerse de las amenazas cibernéticas. Los ciberdelincuentes pueden aprovechar vectores de ataque o vulnerabilidades y dirigirse a organizaciones con una falta de madurez y habilidades en ciberseguridad.

Por ejemplo, un adversario podría utilizar la escasez de habilidades como una oportunidad para llevar a cabo ataques cibernéticos en infraestructuras críticas de otro país durante un conflicto geopolítico.

Proveedores de servicios de TIC transfronterizos como un único punto de falla

Hace referencia a la dependencia de los servicios de TIC proporcionados por proveedores que operan a través de fronteras internacionales. Esta dependencia puede crear un riesgo significativo, ya que cualquier interrupción o compromiso en la infraestructura o servicios de estos, puede tener un impacto generalizado en múltiples sectores y países. Las empresas que ofrecen servicios de TIC transfronterizos actúan como intermediarios críticos para la conectividad y el funcionamiento de servicios esenciales, como el transporte, la energía, las comunicaciones y la banca. Si estas organizaciones se ven comprometidas o experimentan interrupciones, puede haber un impacto significativo en la continuidad de los servicios y la infraestructura crítica. Por ejemplo, un ataque dirigido a un proveedor de servicios de nube transfronterizo podría resultar en la interrupción de servicios en múltiples países, afectando a empresas, gobiernos y ciudadanos. Además, la dependencia de un solo proveedor puede crear un riesgo de monopolio o falta de diversidad en el suministro de servicios, lo que dificulta la resiliencia y la capacidad de respuesta en caso de incidentes.

Esta amenaza destaca la importancia de diversificar y fortalecer la infraestructura y los servicios de TIC, así como establecer mecanismos de cooperación y coordinación entre países para abordar los riesgos asociados con la dependencia de proveedores transfronterizos.

Abuso de la Inteligencia Artificial

Hace referencia al mal uso y manipulación de algoritmos de inteligencia artificial con fines nefastos. Los ciberdelincuentes pueden manipular los algoritmos y los datos de entrenamiento para mejorar actividades ilícitas, como la creación de desinformación y contenido falso, la explotación de sesgos, la recopilación de biometría y otros datos sensibles, el uso de robots militares y la contaminación de la información.

Por ejemplo, los atacantes podrían manipular algoritmos de IA utilizados en plataformas de redes sociales para difundir desinformación y propaganda, manipulando en la opinión pública y recayendo la confianza en las instituciones. Este abuso de la inteligencia artificial plantea desafíos significativos en términos de ética, privacidad y seguridad. En este sentido, es necesario desarrollar mecanismos de control y regulación adecuados para garantizar un uso responsable y seguro de la inteligencia artificial.

Aumento del cibercrimen habilitado por monedas digitales

Hace referencia al aumento rápido del cibercrimen que utiliza monedas digitales como medio de pago. Con la amplia aceptación de las criptomonedas, los ciberdelincuentes organizados han ampliado su alcance y han encontrado nuevas formas de financiar y mejorar sus actividades delictivas. Las criptomonedas permiten a los ciberdelincuentes realizar transacciones de forma anónima y sin la intervención de instituciones financieras tradicionales. Esto les brinda una mayor eficiencia y efectividad en sus esfuerzos delictivos, ya que pueden recibir pagos de forma segura y realizar transacciones sin dejar rastros fácilmente rastreables. Por ejemplo, los grupos de ciberdelincuentes que ofrecen servicios profesionales, como ataques cibernéticos, pueden obtener mejores fondos y recursos debido al aumento en la eficiencia y efectividad de sus actividades delictivas. Esto puede resultar en un aumento de los ataques cibernéticos dirigidos a organizaciones e individuos, lo que puede causar daños financieros e interrupciones en los servicios.

Es importante destacar que el uso de monedas digitales en sí mismo no es una amenaza, pero su adopción generalizada y el anonimato que ofrecen pueden facilitar las actividades delictivas en línea. Por lo tanto, es crucial implementar medidas de seguridad y regulaciones adecuadas para prevenir y combatir el cibercrimen habilitado por monedas digitales.

Explotación de datos de e-salud[4] (y genéticos)

Hace referencia al riesgo asociado a la posible explotación o uso indebido de datos sensibles y/o genéticos recopilados en el ámbito de la salud electrónica por parte de ciberdelincuentes. Con el notable aumento en la cantidad de información genética y de salud accesible para diversas partes interesadas en los sectores público y privado, existe la amenaza potencial que se aprovechen las vulnerabilidades presentes en dispositivos de e-salud y en bases de datos que albergan información sumamente delicada.

Estos datos podrían ser explotados por ciberdelincuentes para atacar a individuos o por gobiernos para controlar a las poblaciones, utilizando enfermedades y diversidad genética como justificación para discriminar a las personas. Además, los datos genéticos podrían ser utilizados de manera abusiva para respaldar actividades de aplicación de la ley, como la policía predictiva o para respaldar un sistema de crédito social más rígido.

Por ejemplo, un adversario podría utilizar el análisis de IA para deducir información sobre los oponentes políticos, utilizando datos como la ubicación, el historial médico y el historial de votación de las personas. Esta correlación de datos personales probablemente solo sea factible con el uso de herramientas de inteligencia artificial. Esta amenaza destaca la importancia de proteger y salvaguardar los datos de e-salud y genéticos, así como de establecer regulaciones y medidas de seguridad adecuadas para prevenir su explotación indebida. Es fundamental garantizar la privacidad y la seguridad de estos datos sensibles para proteger a los individuos y evitar posibles abusos.

Le invitamos a dar lectura al artículo titulado "Hackers ponen a la venta datos de usuarios de importante empresa de análisis genéticos" publicado por el periódico el Tiempo de Colombia de fecha 9 de octubre de 2023.

Manipulación de la cadena de suministro de software de verificación de deepfakes

Hace referencia al riesgo que generan actores malintencionados al manipular los programas de software utilizados para verificar la autenticidad de los deepfakes. A medida que esta tecnología se vuelva ampliamente utilizada, surgirá una demanda urgente de contar con software de verificación que analice videos y voces para verificar la identidad de las personas. Sin embargo, esta demanda urgente puede llevar a que los programadores tomen atajos y no implementen las medidas de seguridad adecuadas en el software de verificación. Esto crea una oportunidad para que los ciberdelincuentes inserten puertas traseras o manipulen el software de verificación para permitir el uso de noticias falsas con fines ilegales o poco éticos, como el acoso, la manipulación de pruebas y la provocación de disturbios sociales.

Por ejemplo, un individuo con intenciones maliciosas podría manipular el software de verificación de deepfakes para facilitar la autenticación de contenidos falsos generados mediante esta técnica, lo que podría tener consecuencias graves en términos de desinformación, daño a la reputación y socavamiento de la confianza en los medios digitales. Esta amenaza destaca la importancia de garantizar la integridad y la seguridad de la cadena de suministro de software, implementando medidas de seguridad adecuadas y realizando auditorías regulares para detectar y prevenir cualquier manipulación o compromiso en el software de verificación de deepfakes.

Ataques utilizando computación cuántica

Hace referencia al riesgo que los ciberdelicnuentes aprovechen los recursos de computación cuántica para atacar las implementaciones existentes de criptografía de clave pública. A medida que la computación cuántica se vuelva más accesible, los atacantes podrían utilizarla para romper los algoritmos criptográficos utilizados para proteger la información confidencial y los sistemas de comunicación.

Los ataques que utilizan computación cuántica podrían comprometer la seguridad de las comunicaciones, la integridad de los datos y la confidencialidad de la información. Por ejemplo, los atacantes podrían recurrir a la computación cuántica para romper los sistemas de encriptación y descifrar datos encriptados previamente, lo cual podría tener graves consecuencias en términos de privacidad y seguridad. Además, existe el riesgo de que los ciberdelincuentes recopilen datos encriptados sensibles en la actualidad, con el objetivo de descifrarlos, una vez que la computación cuántica esté ampliamente disponible.

[4] "*La eSalud representa la digitalización en el ámbito sanitario. Su implementación repercute positiva y directamente en la calidad y la atención sanitaria que recibe el paciente*" Recuperado de: eSalud o eHealth, ¿qué es y cuáles son sus ventajas? | UNIR

Explotación de sistemas no parcheados y desactualizados dentro del ecosistema tecnológico intersectorial abrumado

Hace referencia al riesgo del aprovechamiento de vulnerabilidades presentes en los sistemas que no han sido actualizados o parcheados correctamente. En un entorno tecnológico complejo y en constante evolución, donde hay una gran cantidad de herramientas y servicios que requieren actualizaciones frecuentes, es común que los sistemas queden desactualizados o sin parches de seguridad. Esta situación crea una superficie de ataque que puede ser explotada por un adversario, los cuales pueden aprovechar puntos débiles para obtener acceso no autorizado, obtener información confidencial, realizar ataques de denegación de servicio o llevar a cabo actividades fraudulentas.

La falta de actualizaciones y parches adecuados puede ser especialmente problemática en sectores críticos, como infraestructuras clave, donde la interrupción de los sistemas puede tener consecuencias graves para la seguridad y el funcionamiento de la sociedad en general. Para hacer frente a esta amenaza, es fundamental que las organizaciones implementen prácticas sólidas de gestión de parches y actualizaciones, así como el de mantener un monitoreo constante de los sistemas y la utilización de soluciones de seguridad efectivas para protegerse contra las vulnerabilidades conocidas. Además, es importante promover la concientización y la educación en temas de ciberseguridad para garantizar que los usuarios tengan claro la importancia de mantener su entorno digital asegurado.

Inteligencia Artificial Disruptiva / Mejora de los ataques cibernéticos

Hace referencia al riesgo generado por la inteligencia artificial (IA) al ser utilizada para llevar a cabo ataques cibernéticos de manera sofisticada y efectiva. La IA puede ser utilizada tanto por los ciberdelincuentes o por equipos de ciberseguridad para mejorar sus capacidades y estrategias. Los atacantes pueden utilizar la IA para automatizar y agilizar sus ataques, identificar vulnerabilidades en los sistemas objetivo, desarrollar malware más avanzado y adaptarse rápidamente a las defensas implementadas. Por ejemplo, pueden utilizar algoritmos de aprendizaje automático para realizar acciones de phishing más convincentes y personalizados, o para identificar y explotar debilidades en los sistemas de seguridad. Por otro lado, los equipos de respuesta a incidentes informáticos también pueden utilizar la IA para detectar y prevenir explotaciones, analizar grandes cantidades de datos en busca de patrones y anomalías, con el fin de fortalecer las defensas de los sistemas.

Esta amenaza destaca la necesidad de desarrollar y utilizar herramientas de IA éticas en el ámbito de la ciberseguridad. Es importante garantizar que la IA debe ser implementada con controles que certifiquen su buen uso, además, se requiere una mayor colaboración entre los expertos en ciberseguridad y los desarrolladores de IA para anticipar y contrarrestar las nuevas formas de ataques cibernéticos potenciados por esta tecnología.

Inserción de malware para interrumpir la cadena de suministro de producción de alimentos

Hace referencia al riesgo de insertar malware en los sistemas de producción de alimentos para interrumpir su funcionamiento. Con la creciente automatización y digitalización de la producción de suministros, los atacantes pueden aprovechar las vulnerabilidades en los sistemas informáticos para llevar a cabo una serie de acciones perjudiciales. Por ejemplo, pueden realizar ataques de denegación de servicio en plantas de envasado de provisiones, lo que impide que las operaciones de producción de alimentos continúen. También tienen la capacidad de interferir en las herramientas de producción de alimentos procesados para alterar los compuestos presentes en los productos alimenticios. Esta acción podría desencadenar escasez de alimentos, generar interrupciones económicas e incluso ocasionar situaciones de envenenamiento.

Esta amenaza destaca la importancia de implementar medidas de seguridad sólidas en la cadena de suministro de producción de alimentos. Esto incluye la protección de los sistemas informáticos con soluciones de seguridad actualizadas, la implementación de controles de acceso adecuados y la capacitación y entrenamiento del personal en prácticas de ciberseguridad. Además, es fundamental realizar auditorías regulares de seguridad y pruebas de penetración para identificar y abordar posibles vulnerabilidades en los sistemas.

Incompatibilidad tecnológica de las tecnologías blockchain

Hace referencia al riesgo de incompatibilidad entre las tecnologías blockchain diseñadas por diversos grupos gubernamentales, lo que podría ocasionar fallos, malfuncionamientos, pérdida de datos y la explotación de vulnerabilidades en las interfaces de dichas blockchains. Esta falta de compatibilidad tecnológica surge debido a la desconfianza arraigada en la sociedad hacia esta tecnología, incentivando a cada grupo especializado a buscar una ventaja competitiva

Esta incompatibilidad tecnológica plantea desafíos para la gestión del ecosistema y la protección de datos, fomenta la desconfianza y afecta negativamente al comercio y al crecimiento del PIB[5]. Para hacer frente a esta amenaza, es necesario trabajar en la estandarización y la interoperabilidad de las tecnologías blockchain. Esto implica la colaboración entre los diferentes grupos de desarrollo y la adopción de estándares comunes. Además, se deben implementar medidas de seguridad sólidas en las interfaces de las diferentes blockchains para prevenir la explotación de vulnerabilidades.

Disrupciones en blockchains públicas

Hace referencia al riesgo que presentan las blockchains públicas al sufrir interrupciones y fallas en su funcionamiento. A medida que esta tecnología se vuelve ampliamente utilizada en diversos aspectos de la

[5] *"El producto interno bruto (PIB) es el indicador más utilizado para caracterizar el estado de la economía en su conjunto y representa el resultado final de la actividad productiva dentro de un país. Esta medición es importante porque ofrece información sobre el tamaño de la economía y su desempeño, y sirve para hacer comparaciones frente a otros países"* Recuperado de: https://www.banrep.gov.co/es/glosario/producto-interno-bruto-pib

sociedad, las vulnerabilidades en su seguridad pueden ser explotadas por ciberdelincuentes. Estas interrupciones pueden originarse por diversos factores, como el estancamiento en la seguridad de las cadenas de bloques, la desconfianza acumulada en la tecnología, la falta de compatibilidad tecnológica entre distintas plataformas y la carencia de actualizaciones y mantenimiento adecuado de los sistemas.

Impacto físico de las interrupciones naturales / ambientales en la infraestructura digital crítica

Hace referencia al riesgo desatado por desastres naturales y ambientales que puedan causar interrupciones en la infraestructura digital crítica. Estos eventos pueden incluir terremotos, inundaciones, tormentas, incendios forestales y otros fenómenos naturales que pueden dañar o destruir instalaciones físicas en la que se basa la infraestructura digital. Estas interrupciones pueden tener un impacto significativo en la disponibilidad y el funcionamiento de los servicios digitales críticos, como las redes de comunicación, los sistemas de energía, los sistemas de transporte y otros servicios esenciales. Por ejemplo, los cortes de energía causados por un desastre natural pueden dejar fuera de servicio los centros de datos y los servidores, afectando la conectividad y la capacidad de almacenamiento de datos.

Para hacer frente a esta amenaza, es importante implementar medidas de resiliencia y redundancia en la infraestructura digital crítica. Esto incluye la construcción de instalaciones físicas más robustas y resistentes, la implementación de sistemas de respaldo y recuperación ante desastres y la diversificación de las fuentes de energía y conectividad. Además, se deben establecer planes de contingencia y protocolos de respuesta para garantizar una rápida recuperación después de un evento de interrupción natural o ambiental.

Manipulación de sistemas necesarios para la respuesta de emergencia

Hace referencia al riesgo que puede ser generado en sistemas y dispositivos utilizados en situaciones de emergencia debido a su manipulación, lo que puede afectar negativamente la capacidad de respuesta y la seguridad de las operaciones de emergencia. Por ejemplo, los ciberdelincuentes podrían alterar los sensores conectados a los servicios de emergencia con el fin de sobrecargarlos, lo que complicaría la capacidad de respuesta de grupos de socorro y control, tales como la policía y los bomberos. Esto representa un desafío significativo para la respuesta efectiva ante situaciones de emergencia.

Por otra parte, pueden manipular las alarmas de incendio para causar pánico o dificultar la localización de la emergencia por parte de los equipos de respuesta. Estas manipulaciones pueden tener consecuencias graves, como retrasos en la atención médica de emergencia, dificultades en la coordinación de los servicios de emergencia y la posibilidad que se produzcan daños adicionales debido a la falta de respuesta oportuna. Para hacer frente a esta amenaza, es importante implementar medidas de seguridad sólidas en los sistemas y dispositivos utilizados en situaciones de emergencia. Esto incluye la autenticación y el cifrado adecuado de los sistemas, la implementación de controles de acceso y la capacitación del personal en la detección y respuesta a posibles manipulaciones o compromisos de seguridad.

Referentes de consulta que contribuyen en la reducción de brechas de ciberseguridad relacionadas con estas tendencias

Marco para la mejora de la seguridad cibernética en infraestructuras críticas, Versión 1.1"1, emitido por el Instituto Nacional de Estándares y Tecnología (NIST), este tiene como objetivo fortalecer la seguridad cibernética en sectores críticos y en otras comunidades.[6]

"Top 10 tendencias tecnológicas que marcarán el camino hasta 2030" publicado por Numens1. El informe explora las tendencias tecnológicas clave que tendrán un impacto significativo en la industria y en la configuración del futuro. Entre estas se destacan:

- Computación Cuántica: Según el McKinsey Technology Council, la computación cuántica tiene un valor potencial de más de mil millones de dólares para los próximos 13 años. Esta tecnología avanzada acelera el desarrollo de productos y servicios, reduce costos de hardware y mejora la búsqueda de datos no estructurados.
- Hiperautomatización: Combina tecnologías de optimización, predicción y automatización basadas en inteligencia artificial (IA). Su objetivo es digitalizar procesos empresariales de extremo a extremo, mejorando la eficiencia operativa y acelerando el tiempo de comercialización.
- Conectividad 5G: Se espera que para 2030, el 80% de la población mundial tenga cobertura 5G. Esto impulsará cambios en áreas como la digitalización de la producción, el suministro descentralizado de energía y la monitorización remota de pacientes.
- Arquitectura Cloud Distribuida: La combinación de computación en la nube y edge computing permite reducir la latencia en la conexión entre dispositivos y acelerar la toma de decisiones basada en análisis avanzados.[7]

[6] https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf
[7] Top 10 tendencias tecnológicas que marcarán el camino hasta 2030 (numens.ai)

Recomendaciones y Conclusiones

Algunas Recomendaciones para Reducir el Riesgo Frente a Estas Amenazas

- Implementar medidas de seguridad física en los centros de datos y otros lugares donde se almacena y procesa la infraestructura digital crítica, como sistemas de vigilancia, controles de acceso y protección contra incendios.
- Realizar evaluaciones regulares de riesgos y vulnerabilidades en la infraestructura digital crítica para identificar posibles puntos débiles y tomar medidas correctivas.
- Establecer acuerdos de colaboración con proveedores de servicios de emergencia y agencias gubernamentales para compartir información y coordinar esfuerzos en situaciones de emergencia.
- Implementar sistemas de detección y respuesta de intrusiones para monitorear y proteger la infraestructura digital crítica contra posibles ataques y manipulaciones.
- Realizar simulacros y ejercicios de respuesta a emergencias para evaluar la efectividad de los planes de contingencia y mejorar la preparación de la organización.
- Mantener actualizados los sistemas y dispositivos utilizados en situaciones de emergencia con las últimas actualizaciones de seguridad y parches de software.
- Establecer políticas de gestión de riesgos que incluyan la identificación, evaluación y mitigación de los riesgos asociados con la infraestructura digital crítica.
- Promover la conciencia y la educación en ciberseguridad entre el personal de la organización para fomentar una cultura de seguridad y una respuesta adecuada a las amenazas.
- Establecer mecanismos de supervisión y auditoría para garantizar el cumplimiento de las políticas de seguridad y la detección temprana de posibles manipulaciones o compromisos.
- Implementar soluciones de respaldo y recuperación ante desastres para garantizar la disponibilidad, confidencialidad e integridad de los datos en caso de interrupciones o daños en la infraestructura digital crítica.
- Participar en ejercicios y programas de intercambio de información sobre ciberseguridad a nivel nacional e internacional para mantenerse al tanto de las últimas amenazas y mejores prácticas.
- Establecer alianzas estratégicas con partes interesadas

Conclusión

El informe destaca la importancia de anticiparse a las tendencias emergentes y patrones en el panorama de amenazas de ciberseguridad. También resalta la necesidad de fortalecer las capacidades y competencias en el campo de la ciberseguridad, así como de abordar las vulnerabilidades en áreas como la inteligencia artificial, la cadena de suministro de software y la infraestructura crítica. Además, se menciona la importancia de proteger los datos de salud electrónica y genética, así como de abordar los desafíos relacionados con la manipulación de la inteligencia artificial y los ataques físicos combinados con ciberataques.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:


Correo: csirt@unad.edu.co


Twitter: @csirtunad


Página web: https://csirt.unad.edu.co

Referentes Bibliográficos

[1] https://www.enisa.europa.eu/about-enisa/about/es

[2] https://www.enisa.europa.eu/publications/foresight-challenges

[3] https://news.un.org/es/story/2021/07/1494542

[4] https://www.unir.net/salud/revista/esalud-salud-digital/

[5] https://www.banrep.gov.co/es/glosario/producto-interno-bruto-pib

[6] https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

[7] https://www.numens.ai/es/top-10-tendencias-tecnologicas-que-marcaran-el-camino-hasta-2030/#:~:text=Top%2010%20tendencias%20tecnol%C3%B3gicas%20que%20marcar%C3%A1n%20el%20camino,...%208%208.%20IA%20Aplicada%20...%20M%C3%A1s%20elementos

[8] https://www.eltiempo.com/politica/partidos-politicos/elecciones-regionales-en-colombia-encuestas-falsas-y-manipuladas-de-invamer-819869

[9] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/alarma-por-ciberataque-a-23andme-importante-empresa-de-analisis-geneticos-814057