eti
Tecnologías de la Información
RioCuboFarma

#SIGESTIC23

RESPUESTAS

TALLER PRE-EVENTO

Infraestructuras Inteligentes y Ciberseguridad,

#CIBERSEGURIDADPARATODOS

CREAR VALOR

RESUMEN

¿Cómo crear valor con la ciberseguridad? Reflexiones y retos en un mundo digital y tecnológicamente modificado

Editado por: Global Strategy. Lugar de edición: Granada (España). ISSN 2695-8937

reflexiones y retos

Una de las preguntas frecuentes que se les hace a los ejecutivos de seguridad y control es ¿cómo la ciberseguridad/seguridad genera valor? Esta pregunta que tiene por lo general visiones encontradas, distintas interpretaciones y consideraciones muchas veces sólo económicas (...)

Entender qué es el valor, implica no sólo salir de la zona cómoda de las implementaciones tecnológicas y los términos técnicos, sino entrar en la visión holística de la organización y su dinámica de negocios, para identificar las interconexiones que se tienen entre los procesos, la promesa de valor y las innovaciones tecnológicas que se desarrollan para concretar las expectativas superiores de los clientes. Hablar el lenguaje del valor, el lenguaje de los ejecutivos es encontrar los puentes de conexión entre la ciberseguridad y la agenda estratégica de las empresas: el apetito de riesgo.

(...) Para el ejecutivo de ciberseguridad crear valor es preparar a la organización para rebotar ante cualquier evento, preparar el músculo de prácticas y coordinación para mantener la dinámica empresarial, aun esté amenazada y comprometida por evento adverso.

Crear valor desde la ciberseguridad se convierte necesariamente en un reto de liderazgo en el contexto digital que

CREAR VALOR

RESUMEN

¿Cómo crear valor con la ciberseguridad? Reflexiones y retos en un mundo digital y tecnológicamente modificado

Editado por: Global Strategy. Lugar de edición: Granada (España). ISSN 2695-8937

reflexiones y retos

implica crear mecanismos de absorción y restauración frente a eventos y situaciones naturales como son:

- .las mutaciones del entorno de amenazas,
- la explosión de flujos de información y dispositivos conectados,
- los cambios en las regulaciones,
- las afectaciones a los datos personales,
- la desinformación y los engaños,
- la cibercriminalidad transnacional,

los cuales son habilitados por tecnologías de información y materializados, entre otras cosas, a través de los comportamientos de las personas.

La creación de valor desde el desarrollo de capacidades en ciberseguridad asociado con el "sensar y anticipar" se debe convertir en un nuevo estándar emergente y competitivo, que implica persuadir y conectar a los miembros del directorio empresarial con las nuevas características del riesgo cibernético, que más allá de materializar un producto innovador con tecnología, se requiere crear productos y servicios emergentes, nunca antes probados y desafiantes para el estado del arte de la tecnologías en el momento, que necesariamente tendrán un espacio de aprendizaje, de "error" y de oportunidad que deberá ser construido a la medida y con los grupos de interés.

RANSOMWARE
COMO SERVICIO

CRISTIAN F. BORGHELO

DIRECTOR SEGU-INFO
CONSULTOR EN SEGURIDAD DE LA INFORMACIÓN
ARGENTINA

CUÁLES PUEDEN SER LOS ARCHIVOS MÁS SOSPECHOSOS PARA ESCONDER LA REALIDAD DEL RANSOMWARE

Cualquier tipo de archivo se puede utilizar para propagar ransomware.

Los más comunes siguen siendo los ejecutables pero también se pueden utilizar archivos PDF, HTML, JS, etc para hacerlo y lo mismo aplica también para otros sistemas operativos como Linux, MacOS y VMware.

Más info: https://blog.segu-info.com.ar/2023/05/ransomware-contra-sistemas-de.html

POR QUÉ A VECES LOS DESCIFRADORES NO FUNCIONAN COMO SE ESPERA

Los descifradores son herramientas que rara vez funcionan porque el ransomware profesional y bien desarrollado del último tiempo, no puede descifrarse a menos que se conozca la clave privada. Todos ellos utilizan criptografía asimétrica, lo que hace imposible su descifrado a menos que el delincuente publique las claves o la banda sea detenida.

Los descifradores que funcionan son los de ransomware de principiantes o cuando se cumplen las condiciones anteriores.

CUÁLES SERÍAN ALGUNOS AJUSTES DE CONFIGURACIÓN BÁSICOS PARA MI PC

- Utilizar un sistema operativo actualizado y NUNCA con herramientas crackeadas.
- Utilizar un AV actualizado, aunque sea gratuito, NUNCA crackeado.
- No descargar herramientas de cualquier sitio, sino solamente de lugares oficiales.
- No confiar en soluciones "milagrosas", en Internet nadie regala nada.

Sobre Segu-Info...
Segu-Info es un emprendimiento personal de Lic. Cristian Borghello CISSP - CCSK - CSFPC que brinda información sobre Seguridad de la Información desde el año 2000.
https://blog.segu-info.com.ar/

UNA VISIÓN

DEVSECOPS

SIGNIFICA

integrar la seguridad al desarrollo
de las aplicaciones durante todo el
proceso.

SEGURIDAD INTEGRADA

- Establecer una cultura de seguridad mediante sesiones de sensibilización entorno a temas de seguridad relacionados con la actualidad
- Implementar procesos y procedimientos relacionados con la seguridad alineados a los métodos de producción ágil
- Utilizar herramientas dedicadas y que promueven la automatización

IMPLICA

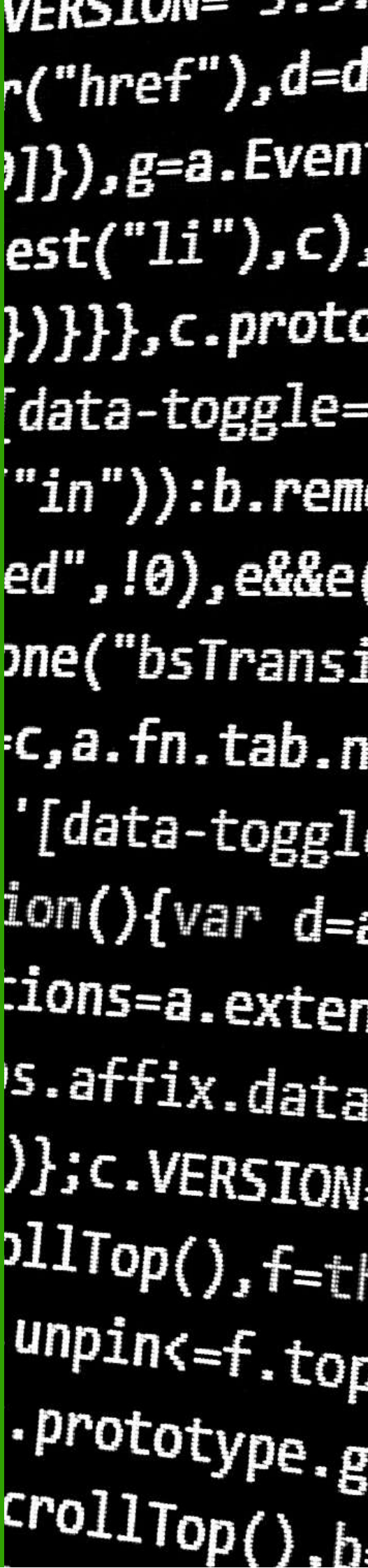
- Pensar desde el principio en la seguridad de las aplicaciones y de la infraestructura.
- Automatizar algunos procesos de seguridad para impedir que se ralentice el flujo de trabajo de DevOps.

ENFOQUE ORGANIZATIVO

- Proceder por capas mediante la introducción gradual de pequeños pasos
- Determinar la tolerancia a los riesgos y realizar un análisis
- de riesgos y beneficios al respecto
- Automatización de las tareas repetidas, pues la ejecución de comprobaciones de seguridad manuales en el proceso puede requerir mucho tiempo.
- Involucrar a todos los trabajadores y contar con el apoyo de la dirección

DEVSECOPS

Responsabilidad compartida e integrada



CAZANDO SOMBRAS EN LA DARK WEB

CUÁL ES LA ESTRATEGIA PARA ORGANIZAR EL TRABAJO EN LA DARK WEB Y SI PUDIERA DEFINIR EN AL MENOS 3 PASOS BÁSICOS

La estrategia depende de cada caso, ya que cada uno de ellos difiere del resto. No obstante, a continuación hago un alto y pues, un resumen en 3 pasos de como me organizo a nivel general:

- Recopilación de información: El primer paso es llevar a cabo una investigación exhaustiva para obtener información sobre las actividades ilegales en la dark web o el caso específico que estés investigando. Esto puede incluir la monitorización de foros y mercados clandestinos, la identificación de patrones y tendencias, y la recopilación de pruebas. También se puede utilizar software especializado para rastrear y analizar transacciones criptográficas, entre otras cosas. Pero este paso se resume en recopilar, recopilar y recopilar, toda la información que puedas sobre tu objetivo.

- Inteligencia y análisis: Una vez recopilada la información, es importante analizarla y extraer inteligencia relevante. Esto implica identificar a los cibercriminales y sus métodos, evaluar el nivel de amenaza que representan y determinar las posibles rutas de investigación. Es fundamental contar con expertos en ciberseguridad y analistas de inteligencia capaces de interpretar los datos recopilados.

- Coordinación y acción: Una vez que se haya obtenido la inteligencia necesaria, es crucial coordinar los esfuerzos entre las fuerzas y cuerpos de seguridad y otros organismos de ciberseguridad en la red. Esto implica compartir información, establecer estrategias de investigación y planificar acciones coordinadas para desmantelar las operaciones criminales. Además, es fundamental contar con la autorización y los recursos necesarios para llevar a cabo acciones legales y detener a los cibercriminales.

CAZANDO SOMBRAS EN LA DARK WEB

QUÉ OTRAS MEDIDAS DE SEGURIDAD PODEMOS INCLUIR DURANTE LA EXPLORACIÓN EN LA DARK WEB?

Estas medidas pueden ayudar a proteger tu identidad y mantener un nivel básico de seguridad:

- Uso de una red privada virtual (VPN)
- Navegador TOR, perfectamente configurado, no por defecto. Hay mucha gente que instala el navegador para acceder a la dark web y lo deja por defecto. Esto no garantiza tu seguridad. Existen diferentes opciones de seguridad y privacidad que te recomiendo eches un vistazo.
- Considera utilizar herramientas adicionales como cortafuegos (firewalls) y software antivirus o EDR actualizado para proteger tu dispositivo contra posibles amenazas. Mantén tu sistema operativo y tus aplicaciones actualizadas con los últimos parches de seguridad.
- No reveles información personal: Evita compartir información personal, como tu nombre real, dirección o datos de contacto, al interactuar en la dark web. Mantén tu identidad separada y utiliza pseudónimos o nombres de usuario alternativos.
- Precaución al hacer clic en enlaces y descargas: Ten cuidado al hacer clic en enlaces o descargar archivos de origen desconocido en la dark web. Los cibercriminales pueden utilizar técnicas de phishing o distribuir malware a través de enlaces y archivos maliciosos.

PRINCIPALES MOTORES DE BÚSQUEDAS PARA ENLACES ONION

Existen muchos, pero alguno de ellos pueden ser, Tor Hidden Service Directories, Torch, The Hidden Wiki, Daniel's Onion Link List, Grams, Ahmia.fi, Candle, Haystak.

Claro está, depende de lo que estés buscando. Mucho cuidado con esto, porque puedes entrar en terreno peligroso.

CÓMO ACCEDER A DATOS ÚTILES Y PRECISOS?

Aquí tienes algunas estrategias y consideraciones importantes, además de las ya mencionadas.

- Fuentes confiables y monitorización: Identifica fuentes confiables de información en la dark web, como foros especializados, mercados clandestinos y comunidades de ciberdelincuentes. Monitoriza estas fuentes regularmente para obtener información sobre actividades delictivas, técnicas utilizadas, nuevos vectores de ataque y tendencias en el panorama cibercriminal.

- Participación activa y construcción de perfiles: Participa activamente en comunidades y foros relevantes en la dark web. Esto implica interactuar con otros usuarios, construir perfiles y ganar confianza. A través de esta participación, puedes obtener información valiosa y establecer contactos que puedan proporcionarte información útil sobre cibercriminales y sus actividades.

- Herramientas de inteligencia y análisis: Utiliza herramientas de inteligencia y análisis para recopilar y procesar datos de manera eficiente. Estas herramientas pueden ayudarte a rastrear transacciones criptográficas, analizar patrones de

CAZANDO SOMBRAS EN LA DARK WEB

comportamiento, identificar conexiones entre actores cibercriminales y realizar análisis forenses digitales.

- Colaboración con organismos de seguridad: Trabaja en estrecha colaboración con agencias de aplicación de la ley, organizaciones de seguridad cibernética y expertos en la materia. Comparte información relevante y colabora en la identificación y seguimiento de cibercriminales en la dark web. La colaboración con profesionales del campo puede proporcionar acceso a herramientas y recursos adicionales.

CÓMO UTILIZAR EL MODELO DE CONFIANZA CERO?

El modelo de confianza cero o Zero Trust, es un enfoque de seguridad que se basa en la premisa de que no se confía automáticamente en ningún usuario o dispositivo, incluso dentro de una red segura. Aquí tienes algunas consideraciones para aplicar este modelo en la investigación en la dark web:

- Autenticación sólida: Implementa una autenticación sólida en todos los sistemas y recursos utilizados durante la investigación. Utiliza autenticación multifactor (MFA) para asegurarte de que solo personas autorizadas puedan acceder a la información y recursos sensibles.

- Cifrado de extremo a extremo: Utiliza el cifrado de extremo a extremo para proteger la confidencialidad de los datos en tránsito. Esto asegura que los datos estén protegidos durante la comunicación y solo puedan ser descifrados por los participantes autorizados.

- Segmentación de redes y privilegios mínimos: Divide las redes en segmentos más pequeños para reducir el riesgo de propagación de amenazas, al menos desde la o las máquinas a través de las cuales entrarás a la dark web. Implementa políticas de privilegios mínimos para limitar el acceso a los recursos

CAZANDO SOMBRAS EN LA DARK WEB

críticos y garantizar que solo los investigadores autorizados tengan los permisos necesarios.

- Monitorización y detección continua: Implementa soluciones de monitorización y detección de amenazas en tiempo real para identificar posibles actividades maliciosas en la dark web. Esto puede incluir sistemas de detección de intrusiones, análisis de comportamiento y herramientas de inteligencia de amenazas.

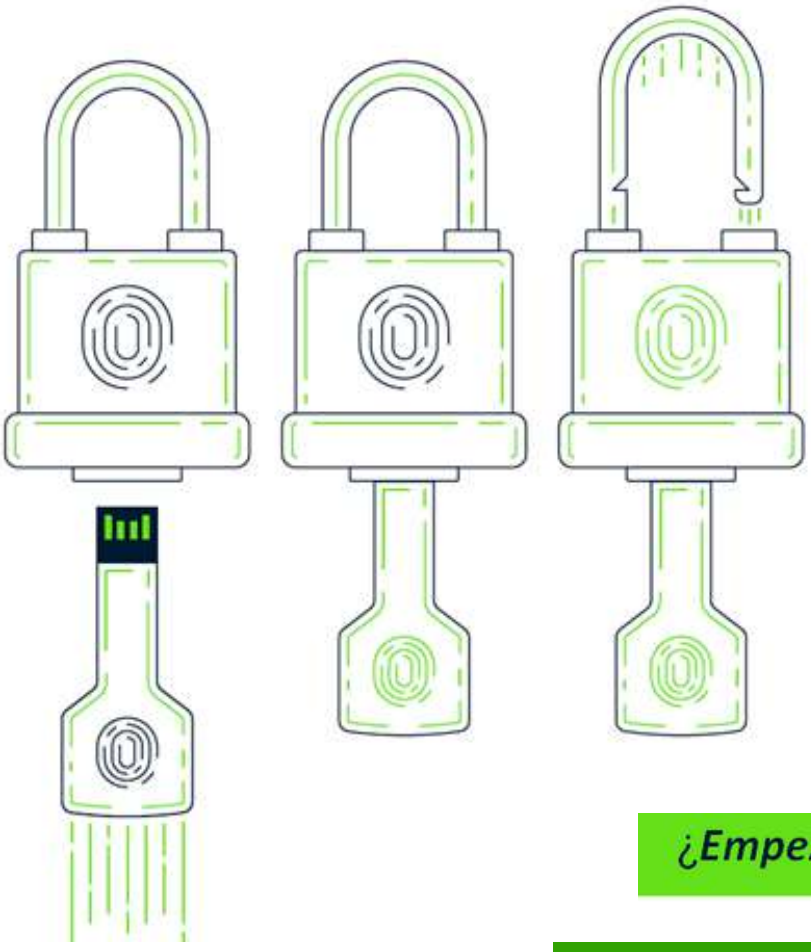
- Aislamiento de entornos sensibles: Considera la posibilidad de utilizar entornos aislados y separados para almacenar y analizar datos sensibles relacionados con la investigación. Esto ayuda a mitigar el riesgo de que los cibercriminales accedan a información confidencial y evita la

contaminación de los sistemas principales. Te lo recomiendo encarecidamente.

- Actualizaciones y parches regulares: Mantén todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad. Esto ayuda a cerrar las posibles brechas de seguridad conocidas y garantiza que los sistemas estén protegidos contra vulnerabilidades conocidas. Es obvio, pero no se hace.

CAZANDO SOMBRAS EN LA DARK WEB

Sobre CiberINseguro.....
CiberINseguro, tu comunidad de Ciberseguridad y Hacking Ético !
de Raúl Beamud, el fundador de la comunidad CiberINseguro
Pentesting, Red & Blue Team, Hacker Ético Experto, y como Perito Informático Forense, Mentor en la National Cyber League de la Guardia Civil.inalista para estar dentro de los TOP 100 Hackers de EC-Council.
https://ciberinseguro.com/



¿Empezamos a trabajar juntos?

LAS CLAVES DEL ÉXITO PARA LA GESTIÓN DE RIESGOS

UN E-BOOK EDITADO POR
ISOTOOLS EXCELLENCE

La ISO 27001 establece un Sistema de Gestión de Seguridad de la Información, cuyo elemento más importante es la Gestión de los Riesgos.

Dentro de la Gestión de Riesgos podemos identificar dos etapas principales: Análisis y Tratamiento, que incorpora Metodologías Específicas para:

- Identificación de Activos de información con una categorización
- Identificacion de Amenazas y Vulnerabilidades basado en un catálogo de amenazas
- Cálculo del Riesgo, a partir de la definición de parametros como la probabilidad de materializacion de una amenaza y el impacto en la organizacion.
- Establecimiento de Controles, mediante el establecimiento de un Plan de Contingencias.

CUÁL ES EL MEJOR MOMENTO PARA DESARROLLAR UN CIBEREJERCICIO ?

Los ejercicios son precisamente para entrenar al personal y se deben basar en lo que cada organización tenga, tanto de Equipo de Respuesta de Incidentes o de Seguridad como de Personal externo.
Para que se haga una idea, las prácticas de simulación de huracanes las hacen sin importar cuantos desastres tengan asignados, asi mismo es esto.
Justamente lo que le permite a la empresa es ver realmente que pasaría en caso de un ataque y que puede verse afectado y como mejorar su posición.

QUÉ PASA CUANDO UN CIBEREJERCICIO TRASPASA LAS FRONTERAS DE LA ORGANIZACIÓN INVOLUCRANDO A TERCEROS CON SERVICIOS CONTRADTADOS ?

He trabajado en varios así , se tiene que coordinar con los terceros una Respuesta o se simula cual creen que sería la Respuesta del Tercero, Lo importante es ver y entender cómo es la interacción en el momento de un incidente y si todos saben qué hacer y con quién comunicarse.

ENTRENANDO LA RESPUESTA DE INCIDENTES

POR SU EXPERIENCIA QUÉ CAMBIOS SE REALIZAN A CORTO PLAZO TRAS SUSPENDER UN CIBEREJERCICIO ?

Mi experiencia está más del que confecciona los ejercicios o estoy en la atención del incidente, asi que no siempre veo lo que sucede después. Pero , usualmente se mejoran los Planes de Respuesta a incidentes (haciéndose más reales), la organización se vuelve más consciente y se mejora la interacción con terceras partes.

Más info: https://www.one-esecurity.com/news/article_irplan.html

Sobre Diego Espitia, +de 15 años de experiencia
CEH - Certicated Ethical Hacker, Auditor Interno ISO 27001:2013, Seguridad OTSeguridad OT Telefónica Tech Cyber Security & Cloud
Profesor Y Ponente Black Hat USA and Europe, AtHack Arabia
https://www.one-esecurity.com

SIGESTIC'23

TALLER PRE-EVENTO INFRAESTRUCTURAS Y CIBERSEGURIDAD

#ABUENPUERTO
#SIGESTIC23

csirt-bcf

equipo de respuesta a incidentes de ciberseguridad
BioCubaFarma

HTTPS://CSIRT.BIOCUBAFARMA.CU/

#SIGESTIC23

RESPUESTAS

TALLER PRE-EVENTO

Infraestructuras Inteligentes y Ciberseguridad,

#CIBERSEGURIDADPARATODOS