SIGESTIC>23 TALLER INFRA-CIBER OCT-2023

PREGUNTAS

RESPUESTAS

#ABUENPUERTO

#CIBERSEGURIDADPARATODOS

DESAFÍOS EN LA INNOVACIÓN
EN CIBERSEGURIDAD

Ing . Federico Pacheco

I+D+i Manager en BASE4 Security (Argentina-España). Especialista en Ciberseguridad con 20 años de experiencia en la industria, y formación de grado en ingeniería electrónica.

QUÉ ELEMENTOS SE HAN DE TENER EN CUENTA PARA QUE LA INNOVACIÓN EN CIBERSEGURIDAD SE DEFINA COMO UN DIFERENCIADOR ESENCIAL EN EL MODO EN QUE LA EMPRESA CREA VALOR Y OBTIENE INGRESOS Y BENEFICIOS.

La innovación en ciberseguridad se convierte en un diferenciador esencial para una empresa cuando se abordan varios aspectos clave. En primer lugar, es clave tener comprensión de las amenazas y riesgos específicos que enfrenta la organización. Además, se debe fomentar una cultura de ciberseguridad en todos los niveles de la empresa, respaldada por inversiones en tecnología y recursos adecuados. La colaboración con otros actores, la personalización de la estrategia de seguridad y la automatización de procesos son elementos esenciales. Cumplir con regulaciones, educar de manera continua a los empleados, gestionar incidentes eficazmente y realizar evaluaciones y mejoras constantes son prácticas que ayudan a que la innovación en ciberseguridad se traduzca en la creación de valor y la obtención de beneficios para la organización.

Finalmente podemos decir que un modelo de creación de valor es aquel que tenga como eje fundamental el empleo de la psicología cognitiva para el análisis de los perfiles de amenazas, un modelo de beneficio ajustado a determinar los impulsores claves de la rentabilidad de una inversión en innovacion y los ingresos asociados a la nueva propuesta de Cibereguridad y por último la lógica de los negocios, pensada como la vía por la cual la empresa alcanzará sus objetivos de beneficio y crecimiento.

DESAFÍOS EN LA INNOVACIÓN
EN CIBERSEGURIDAD

Ing . Federico Pacheco

I+D+i Manager en BASE4 Security (Argentina-España). Especialista en Ciberseguridad con 20 años de experiencia en la industria, y formación de grado en ingeniería electrónica.

CONSTRUIR UN NEGOCIO EN CONDICIONES DE PROSPERIDAD Y OPORTUNIDADES SON OBJETIVOS CLAVES PARA UN ECOSISTEMA EMPRENDEDOR. CUÁLES DE LOS SIETE DESAFÍOS PLANTEADOS RESPONDEN AL 70% DE LAS VARIABLES QUE IMPACTAN MÁS PROFUNDAMENTE EN UNA INNOVACIÓN EN CIBERSEGURIDAD.

Para que funcione positivamente un ecosistema emprendedor, la mirada debe centrarse en definir que variables aportan a mi contexto de innovación y desarrollo. Mi abanico de variables principales son: Política, Finanzas, Cultura, Soporte, Capital Humano y Mercados, luego las de mayor peso son Política, Finanzas y Cultura y aquí en estas 3 ubicaría a los desafíos de innovación en ciberseguridad: la mentalidad adecuada, los entornos complejos y aprender a tomar riesgos sean de mayor impacto, pero ninguna de las demás deben descartarse

EN EL DESARROLLO DE SOLUCIONES INNOVADORAS EN CIBERSEGURIDAD QUÉ ARISTA ES LA MÁS TRABAJADA Y POR QUÉ: SEGURIDAD REACTIVA O SEGURIDAD PROACTIVA

La seguridad proactiva tiene más espacio de innovación, dado que se viene trabajando mucho más en la historia en las reactivas.

DESAFÍOS EN LA INNOVACIÓN
EN CIBERSEGURIDAD

Ing . Federico Pacheco

I+D+i Manager en BASE4 Security (Argentina-España). Especialista en Ciberseguridad con 20 años de experiencia en la industria, y formación de grado en ingeniería electrónica.

CÓMO IMPACTAN LAS TENDENCIAS EN CIBERSEGURIDAD EN LOS PROCESOS DE INNOVACIÓN COMO HABILITADOR CLAVE EN EL CRECIMIENTO DE UNA SOCIEDAD ENCAMINADA A LA DIGITALIZACIÓN

Las tendencias en ciberseguridad desempeñan un papel crucial como habilitadores clave en la sociedad digital. El aumento de las ciberamenazas impulsa la innovación en soluciones de seguridad más sofisticadas, mientras que la protección de datos y la privacidad son prioritarias debido a regulaciones como GDPR. La inteligencia artificial y el aprendizaje automático se utilizan para detectar amenazas, y las soluciones en la nube y la autenticación multifactor se están expandiendo. La colaboración en ecosistemas de seguridad y la gestión en tiempo real de amenazas también son áreas de innovación esenciales para garantizar la confianza y la protección en la sociedad digitalmente avanzada.

A VECES SOLO SE VE LA INNOVACIÓN EN CIBERSEGURIDAD COMO ALGO TECNOLÓGICO, COMO PLANTEARSE TAMBIÉN LA IDEA FUERA DE ESTE ENTORNO.

Lo concerniente a personas es transversal a cualquier entorno de innovación, solo uno de los desafíos planteados corresponden especificamente a ciberseguridad (el del poco personal especializado).

ARQUITECTURAS DEFENDIBLES
EN ICS/OT

Ing . Diego Samuel Espitia

Senior Technical Consultant para CyberEx and Incident Response Senior Technical Consultant para CyberEx e Incident Response One eSecurity (Colombia). Ingeniero Electrónico de profesión, hacker por pasión. 15 años de experiencia en procesos de ciberseguridad.

LA ADOPCIÓN DE UNA GESTIÓN DE VULNERABILIDADES BASADA EN RIESGOS ES UNO DE LOS CONTROLES MOSTRADOS. CÓMO PRIORIZAR LA GESTIÓN DE UNAS SOBRE OTRAS, A PARTIR DE LA DEFINICIÓN DE DICHAS VULNERABILIDADES.

Priorizar, ahí esta la clave, diría que lo primero es gestionar las vulnerabilidades que se suceden donde más tráfico e interconexión hay entre los puntos convergentes IT/OT,y después las joyas de la corona y otros sistemas que pudieran considerarse críticos en cada uno de los niveles del Modelo Purdue. Ahora bien, si consideramos en primera instancia que la solución de las vulnerabilidades en mayor % pueden “parchearse”, el análisis de tu activos ubicaría los activos por prioridad de parcheo, gestionarndo las vulnerabilidades sobre estos. Es un trabajo no solo de IT o de seguridad, sino de equipo, para determinar que es o no vital en un proceso.

CUÁLES PUDIERAN SER LOS ELEMENTOS COMUNES A TENER EN CUENTA PARA DEFINIR UNA ARQUITECTURA DEFENDIBLE.

Una arquitectura que sea defendible o no, a mi enteder depende de la cantidad de riesgo tolerado por el diseño y la implementación de dicha propuesta. Eso sin contar que no existe una arquitectura de seguridad perfectamente segura y es que no depende exclusivamente de las normativas o regulaciones o buenas prácticas, lo que marca el ritmo es el desempeño de las organizaciones. Lo veo como la capacidad de adoptar una

ARQUITECTURAS DEFENDIBLES
EN ICS/OT

Ing . Diego Samuel Espitia

Senior Technical Consultant para CyberEx and Incident Response Senior Technical Consultant para CyberEx e Incident Response One eSecurity (Colombia). Ingeniero Electrónico de profesión, hacker por pasión. 15 años de experiencia en procesos de ciberseguridad.

postura cibernética defendible, ante situaciones hostiles o de incidentes de seguridad, añadiendo como mínimo una buena segmentación, un robusto sistema de control de acceso y un monitoreo de cada activo.

QUÉ OTROS MARCOS DE SEGURIDAD, SE PUEDEN APLICAR EN EL DISEÑO DE ARQUITECTURAS DEFENDIBLES EN ICS/OT.

En ICS casi que cada tipo de industria tiene sus marcos. Lo indicado es seguir la IEC 62443 que está enfocada en ciberseguridad y busca ser aplicable a cualquier tipo de industria. Pero agregaría uno por el cual me guío NIST SP 800-82r3 ipd, que describe cómo mejorar la seguridad de los sistemas de tecnología operativa (OT) al mismo tiempo que atiende a sus requisitos de rendimiento, confiabilidad y seguridad.

También pudiéramos incorporar al Modelo Purdue ISA 95/IEC 62264.

CUÁLES SON LOS PRINCIPALES BENEFICIOS ASOCIADOS A SU IMPLEMENTACIÓN.

EL principal beneficio es que en caso de un incidente no se compromete toda la operación, la gestión de datos es más simple y estructurada, además que permite la identificación temprana de comportamientos anómalos. Pudiera decirse además que estamos ante una seguridad mejorada, que el riesgo de ocurrencias de incidentes de seguridad disminuye y que la puesta en marcha de una arquitectura defendible pues apuesta por el cumplimiento normativo de estándares que regulan y establecen las mejores prácticas hacia la protección de la industria.

ARQUITECTURAS DEFENDIBLES
EN ICS/OT

Ing . Diego Samuel Espitia

Senior Technical Consultant para CyberEx and Incident Response Senior Technical Consultant para CyberEx e Incident Response One eSecurity (Colombia). Ingeniero Electrónico de profesión, hacker por pasión. 15 años de experiencia en procesos de ciberseguridad.

CÓMO APROVECHAR LA INTELIGENCIA SOBRE AMENAZAS EN TODO SU DISEÑO, DESARROLLO Y OPERACIONES A PARTIR DE QUE SE ASUMA QUE LA EMPRESA TAMBIÉN DEBE SER DEFENDIBLE

La inteligencia de amenazas es fundamental para la definición de estrategias de defensa con la base de comportamientos conocidos, generación de escenarios viables de ataque, generación de alertas preventivas, conocimiento de incidentes en el sector y enfoque de prioridades, así que para que una arquitectura defendible sea escalable y actualizable es fundamental usar la inteligencia de amenazas. Para que una Empresa sea Defendible eficientemente se traduce en que los controles propuestos pues tengan menos pasos. Al final quienes defendemos, evaluamos cuales son los controles más pertinentes para los indicadores establecidos por quienes diseñan, construyen, ejecutan. En otras palabras, nosotros, a partir del seguimiento de los controles, somos quienes podemos planificar mejoras futuras para esas arquitecturas.

SI TUVIERA QUE DEFINIR UN CICLO DE VIDA PARA ARQUITECTURAS DEFENDIBLES, CUÁLES SERÍAN LAS ETAPAS PROPUESTAS

Yo considero que es un PHVA como muchos de calidad o de procesos, pero lo importante es que se mantenga una vigilancia sostenida en Threat hunting, en Intenligencia cibernética y en feedback de las mismas medidas. Pensando siempre como defenderte, 3 cosas que he aprendido : visibilidad, manejabilidad, y supervivencia, de esta forma aprovechas al máximo tu diseño de la arquitectura. Es un ejercicio para reaprender.

TRATAMIENTO DE INCIDENTES

Lic . Cristian F. Borghello

Director Segu-Info - Consultor en Seguridad de la Información (Argentina). Licenciado en Sistemas, desarrollador, Certified Information Systems Security Professional, Certificate of Cloud Security Knowledge y Cyber Security Foundation y fue Microsoft MVP Security (Most Valuable Professional) durante 10 años.

CÓMO ALTERA LA ADICIÓN DE LA FUNCIÓN DE GOBERNANZA A LAS CINCO FUNCIONES ESTABLECIDAS EN EL NIST CYBERSECURITY FRAMEWORK (CSF), EN CUANTO A CAPACIDADES DE CIBERSEGURIDAD DE EFECTIVIDAD EN EL TRATAMIENTO DE INCIDENTES.

Al sumarse gobernanza se agrega un punto importante y ya considerado en otros frameworks en donde tiene que haber una responsabilidad "política" de garantizar la ciberseguridad de la organización y potenciar el resto de los pilares.

POR SU EXPERIENCIA QUÉ FRAMEWORK DE RESPUESTA A INCIDENTES SERÍA EL MÁS CONVENIENTE EMPLEAR (SANS VS NIST, SEGÚN LA FILOSOFÍA DE CADA UNO), TENIENDO EN CUENTA QUE LA PRINCIPAL DIFERENCIA ENTRE AMBOS SON LOS PASOS DE CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN.

Ambos son importantes, pero creo que lo más adecuado es que cada organización cree su propio modelo en base a su experiencia, forma de trabajo, incidentes pasados, etc

TRATAMIENTO DE INCIDENTES

Lic . Cristian F. Borghello

Director Segu-Info - Consultor en Seguridad de la Información (Argentina). Licenciado en Sistemas, desarrollador, Certified Information Systems Security Professional, Certificate of Cloud Security Knowledge y Cyber Security Foundation y fue Microsoft MVP Security (Most Valuable Professional) durante 10 años.

CÓMO AYUDAN LOS INDICADORES DE COMPROMISO EN LAS OPERACIONES DIARIAS Y CÓMO RECOPILARLOS PARA LA GENERACIÓN DE UN INFORME FINAL.

Los IoC son fundamentales en la detección de incidentes y actualmente la principal fuentes son los SIEM y herramientas similares que tienen feeds automáticos que se actualizan en tiempo real.

QUÉ HERRAMIENTAS OPEN SOURCE RECOMENDARÍA PARA CUBRIR EL CICLO COMPLETO EN EL TRATAMIENTO DE UN INCIDENTE.

Algunas tools de monitoreo pueden ser Wazuh, TheHive, Misp, Cortex, Snort, Suricata, BroIDS, OSSEC, Nagios.

MODELO DIAMANTE

Ms.C . Rubén Bernardo Guzmán Mercado

IT Cordinator, Information Technology and Cybersecurity Specialist, IT Manager (México). Máster en tecnologías de la información, se especializa en ciberseguridad, con 22 años de experiencia en empresas de orden mundial.

QUÉ CRITERIOS ESPECÍFICOS DEBO TENER EN CUENTA PARA HACER UNA INVESTIGACIÓN PROFUNDA SOBRE EL DESENVOLVIMIENTO DEL ADVERSARIO EN LA INFRAESTRUCTURA AGREDIDA O VÍCTIMA.

Como primer paso, debemos considerar que nuestras defensas en cualquier momento pueden ser vulneradas, el camino y desenvolvimiento del adversario depende de las capas de seguridad, entonces para ello debemos tener muy bien controladas dichas capas, generalmente no anticipamos ataques con el modelo diamante, con él podemos saber donde se encuentran las brechas y cerrarlas, cuando haces esto vas paso a paso en el camino del adversario y tu investigación es profunda y efectiva ya que te permitirá reforzar tu ciberseguridad completa, aún cuando puede ser por evento, la mayoría de las veces, ya en un ámbito más avanzado puedes llegar hasta prevenir o mitigar ataques a tu entorno.

CÓMO ESTE MODELO DE ANÁLISIS DE INTRUSIÓN MEJORA LA CALIDAD DE LOS IOC.

El saber el camino del adversario es importante en el sentido que nos permite reforzar la ciberseguridad cerrando brechas, en cuanto la calidad de los IoC, bueno este un término forense que se refiere a la evidencia en un dispositivo que señala una brecha de seguridad, en la práctica se obtienen después del evento o eventos, este proceso está vinculado estrechamente a los dispositivos y muy común verificar los datos de los IOC de manera regular para detectar actividades inusuales y vulnerabilidades, recuerden la tendencia de monitoreo es encontrar actividad anómala e inusual.

MODELO DIAMANTE

Ms.C . Rubén Bernardo Guzmán Mercado

IT Cordinator, Information Technology and Cybersecurity Specialist, IT Manager (México). Máster en tecnologías de la información, se especializa en ciberseguridad, con 22 años de experiencia en empresas de orden mundial.

POR QUÉ DIAMANTE Y NO KILL CHAIN O MITRE ATT&CK.

Todas estas técnicas tienen algo en común, es la de saber como fue que nos vulneraron, que camino siguieron y tratar de identificar que se llevaron, yo no pondría una técnica antes que otra, las 3 son buenas, lo importante es con cual en la practica observas mejores y mas reales resultados, la infraestructura y la capacidad del atacante es significativa si llegas pronto a identificarlas y ver la posible ruta del atacante y en un grado más avanzado prevenir o mitigar mas proactivamente los eventos que se presenten.

SE COMENTA QUE EL MODELO DIAMANTE POSEE UNA CAPACIDAD ÚNICA PARA SALVAGUARDAR LAS INFRAESTRUCTURAS DIGITALES A PARTIR DEL DESARROLLO DE ESTRATEGIAS DE MITIGACIÓN PREVENTIVAS, LUEGO COMO SERÍA LA PLANIFICACION DE UNA SEGURIDAD CON DEFENSA ACTIVA, BASADO EN EL CIBERENGAÑO.

En estas técnicas tu puedes ver tendencias y prevenir desde tu infraestructura hasta la capacitación a tus usuarios, tengan presente que son los objetivos primarios en un ataque con ciberengaños, consideremos una cosa, el factor humano es la brecha más grande que puedes llegar a tener, tu estrategia primaria es preventiva, concientizando a los usuario esta defensa es activa porque es muy continua y debe estar actualizada, porque no importa que tan

MODELO DIAMANTE

Ms.C . Rubén Bernardo Guzmán Mercado

IT Cordinator, Information Technology and Cybersecurity Specialist, IT Manager (México). Máster en tecnologías de la información, se especializa en ciberseguridad, con 22 años de experiencia en empresas de orden mundial.

grandes sean las aplicaciones y hardware para ciberdefensa, si un usuario con un clic puede generar una brecha, por otra parte si implementas demasiados mecanismos de ciberseguridad puedes volverte inoperante.

Si haces un simulacro de algún escenario con el modelo diamante, te sorprenderá el resultado mediante vayas pasando tus defensas.

SIGESTIC>23 TALLER INFRA-CIBER OCT-2023

PREGUNTAS

RESPUESTAS

#ABUENPUERTO

#CIBERSEGURIDADPARATODOS