UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

FACULTAD 2

El empleo de las buenas prácticas del CERT para el mejoramiento de la Ciberseguridad de las instituciones

Seminario de Seguridad en el Desarrollo de Software

Grupo:2304

Integrantes:

Erick Carlos Miralles Sosa:erickcms@estudiantes.uci.cu
Marcos Daniel Artiles Delgado:marcosdad@estudiantes.uci.cu
Sabrina D'Lory Ramos Barreto:sabrinadlrb@estudiantes.uci.cu
Keylan Valdés García:keylanvg@estudiantes.uci.cu
Sheila Hernández Falcón:sheilahf@estudiantes.uci.cu

Introducción

El gusano Morris, lanzado por Robert Tappan Morris el 2 de noviembre de 1988, se destacó como el primer gusano de la historia, infectando aproximadamente el 10% de los servidores conectados a la red. La magnitud de este evento significativo llevó a la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) a tomar medidas serias. En respuesta, no solo establecieron protocolos y directrices específicos, sino que también dieron origen a los Equipos de Respuesta ante Emergencias Informáticas, conocidos como CERT (Computer Emergency Response Teams).

Los CERT, también identificados como CSIRT (Computer Security Incident Response Teams) en términos europeos, representan un grupo selecto de profesionales altamente especializados en la seguridad informática de una organización. Su tarea principal radica en vigilar de forma continua la integridad y seguridad de las redes y sistemas informáticos, así como implementar planes de acción para abordar eficazmente cualquier incidente informático que pueda surgir.

En el panorama actual, con el incremento exponencial de los ciberataques dirigidos a las organizaciones, la relevancia y necesidad de los equipos CERT se vislumbra más crítica que nunca. Esta investigación se propone como objetivo principal caracterizar las mejores prácticas adoptadas por los CERT, incluyendo normativas, resoluciones y estándares establecidos para fortalecer la ciberseguridad y la respuesta ante incidentes en las empresas.

Desarrollo

Los equipos de Respuesta ante Emergencias Informáticas(CERT) para encargarse de la vigilancia efectiva de la ciberseguridad realizan el Plan de Respuesta a Incidentes(IRP) rigiéndose por variedad de estándares y protocolos dependiendo de cada país. Pero los más comunes son los estándares ISO, FIRST y NIST.

El Instituto Nacional de Estándares y Tecnología, , es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos, las cuales rige normas a cumplir por los CERT como son(Wilbur L. Ross,2018):

- **Marco de Ciberseguridad del NIST (NIST Cybersecurity Framework):** Es una guía que proporciona un conjunto de mejores prácticas, estándares y controles para ayudar a las organizaciones a gestionar y mejorar su postura de ciberseguridad. El marco se basa en cinco funciones principales: identificar, proteger, detectar, responder y recuperar.
- **Estándares del NIST para la Seguridad de la Información (NIST SP 800 series):** Esta serie de publicaciones proporciona pautas y recomendaciones para diversos aspectos de la seguridad de la información, como la gestión de contraseñas, el cifrado, la autenticación, la gestión de incidentes y muchos otros temas relacionados con la ciberseguridad.
- **Guía para la Evaluación y Mitigación de Vulnerabilidades del NIST (NIST SP 800-53A):** Esta guía proporciona un enfoque detallado para evaluar y mitigar las vulnerabilidades en los sistemas de información. Incluye una lista exhaustiva de controles de seguridad que pueden implementarse para proteger los sistemas contra amenazas.

Por otro lado también con objetivo de garantizar un correcto trabajo de los CERT emplean lo recomendado por FIRST.La cual es la principal

organización mundial que fomenta la respuesta de forma coordinada y colaborativa a incidentes de seguridad y promueve acciones de prevención. Surgió en 1990 a causa de dos grandes incidentes de seguridad informática ocurridos en los años anteriores El “Morris Worm”, en noviembre de 1988,El “Wank Worm”, en octubre de 1989.(Cyber Zaintza,2022).

El FIRST recomienda las siguientes estrategias para evitar posibles incidentes:

- Identificar con claridad qué persona lidera la gestión de incidentes.
- Gestionar las posibles brechas y fugas de información.
- Asegurar el apoyo legal y de las Administraciones públicas.
- Estudiar los requisitos de textos legales como, por ejemplo, el RGPD.
- Realizar diversos simulacros y ensayos.
- Trabajar la forma y el tiempo de la respuesta. Es muy importante saber comunicar el problema.
- Comunicar con sinceridad y claridad.
- Estudiar y documentarse acerca de posibles problemas, nuevas vulnerabilidades.
- Compartir los aprendizajes propios con el resto del equipo.

Otro de los estándares que implementa son los regidos por La Organización Internacional de Normalización(ISO) la cual es una organización para la creación de estándares internacionales principalmente la ISO-IEC 27001 y la ISO/IEC 27035

ISO-IEC 27001: Establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) en una organización.

ISO/IEC 27035: Establecer un enfoque estructurado para la gestión de incidentes de seguridad de la información en una organización.

Es necesario cumplir estrictamente estas medidas, el cumplimiento de los requisitos de funcionalidad y desempeño explícitamente establecidos, de los

estándares de desarrollo explícitamente documentados, y de las características implícitas que se espera de todo software desarrollado. La anterior definición, expuesta por Pressman (2005), resalta que los estándares especificados definen un conjunto de criterios de desarrollo que guían la forma en que se aplica la ingeniería del software.

Por lo tanto si no se siguen esos criterios, casi siempre habrá falta de calidad se debe tener en cuenta que la seguridad en el desarrollo de software también forma parte actualmente en la calidad del mismo. Las empresas y organizaciones que no toman medidas adecuadas para proteger la información de sus clientes y usuarios podrían enfrentarse a multas y demandas legales y por tanto a la pérdida de confianza como empresa u organización. La implementación de normas y estándares de seguridad en el desarrollo de software ayuda a prevenir la presencia de vulnerabilidades que podrían ser explotadas por ciberdelincuentes para acceder a datos sensibles o comprometer la integridad del sistema y conlleva a una reducción de riesgos y mejora continua.

Buenas prácticas

Una de las buenas prácticas que se recomiendan son las MANRS(acrónimo de "Mutually Agreed Norms for Routing Security" (Normas Mutuamente Acordadas para la Seguridad en el Enrutamiento) iniciativa global comunitaria dirigida a mejorar la seguridad y la estabilidad de Internet mediante el fortalecimiento de la infraestructura de enrutamiento en línea.Todo esto con el fin de mitigar vulnerabilidades, amenazas como el envenenamiento de rutas, los ataques de secuestro de prefijos, entre otros.

MANRS define cuatro acciones simples pero concretas que los operadores de red deben implementar para mejorar en gran medida la seguridad y confiabilidad de Internet. Entre estas se incluyen:

- **Filtrado:** definir una política de enrutamiento clara e implementar un sistema para garantizar que los anuncios a las redes adyacentes sean correctos.
- **Antisuplantación:** habilitar la validación de la dirección de origen e implementa la antisuplantación para evitar que paquetes con direcciones IP de origen incorrectas entren y salgan de la red.
- **Coordinación:** mantener información de contacto actualizada y accesible a nivel mundial para ayudar con la respuesta a incidentes.
- **Validación global:** publicar datos que permitan a otros agentes validar la información de enrutamiento a escala global. Las acciones de MANRS definen los resultados en lugar de métodos específicos. Esto permite que la implementación cambie con la tecnología y ayuda a establecer las acciones de MANRS como mejores prácticas.

Etapas del ciclo de vida

Las normas y estándares de programación segura CERT (Computer Emergency Response Team) del CERT Coordination Center son una herramienta invaluable para garantizar la seguridad y la fiabilidad del software. Estas normas proporcionan pautas detalladas para el desarrollo de software seguro, abordando temas como el manejo de memoria, la gestión de errores, la autenticación y la autorización, entre otros. La aplicación de estas normas puede adaptarse a diferentes etapas del ciclo de vida del desarrollo de software, desde la concepción y el diseño hasta la implementación y el mantenimiento.

En las primeras etapas del ciclo de vida del desarrollo de software, como la planificación y el diseño, es crucial considerar los principios de programación segura establecidos por las normas CERT. Durante la fase de planificación, se deben identificar los requisitos de seguridad y definir los controles que se implementarán para cumplir con las normas. Al alinear los

diseños con las normas, se puede garantizar que las vulnerabilidades potenciales se aborden desde el principio del proceso de desarrollo.

Durante la fase de implementación, los desarrolladores deben seguir de cerca las pautas específicas de las normas CERT Secure Coding Standards para garantizar que el código se escriba de manera segura y robusta. Esto incluye utilizar prácticas de codificación segura, como la gestión adecuada de la memoria, la validación de datos de entrada y la prevención de vulnerabilidades comunes, como los desbordamientos de búfer o las condiciones de carrera.

Además, en la fase de pruebas, se deben llevar a cabo pruebas de seguridad exhaustivas para identificar posibles debilidades en el software que puedan estar en conflicto con las normas CERT. Estas pruebas son fundamentales para asegurarse de que el software cumple con las expectativas de seguridad establecidas por las normas.

En la etapa de mantenimiento, se debe continuar monitoreando y actualizando el software de acuerdo con las últimas versiones de las normas CERT Secure Coding Standards. Dado que las amenazas cibernéticas evolucionan constantemente, es crucial adaptarse a las actualizaciones de las normas para mantener la seguridad del software a lo largo del tiempo.

En cuanto a la adaptabilidad de las normas CERT a diferentes tipos de proyectos y tecnologías, es importante destacar que estas normas son flexibles y pueden aplicarse a una amplia gama de entornos de desarrollo. Ya sea que se trate de aplicaciones web, aplicaciones móviles, sistemas embebidos o cualquier otro tipo de proyecto de software, las pautas CERT Secure Coding Standards pueden adaptarse para abordar los requisitos específicos de cada entorno.

Ventajas

Entre las ventajas de seguir los estándares de codificación segura del CERT se encuentran:

1. **Mejora de la seguridad:** Al seguir las directrices y recomendaciones del CERT, se reducen las vulnerabilidades en el código y se mejora la seguridad de las aplicaciones y sistemas.

2. **Reducción de riesgos:** La implementación de buenas prácticas de codificación segura ayuda a reducir los riesgos de ataques y brechas de seguridad.

3. Conformidad con regulaciones: Cumplir con los estándares de codificación segura del CERT puede ayudar a cumplir con regulaciones y normativas relacionadas con la seguridad de la información**.**

4. .**Mejora de la calidad del código:** Al aplicar las recomendaciones del CERT, se promueve una mejor calidad en el código, lo que puede facilitar su mantenimiento, reducir errores y mejorar la escalabilidad de las aplicaciones.

5. **Alineación con buenas prácticas de la industria:** Los estándares de codificación segura del CERT están basados en buenas prácticas de la industria de la seguridad informática, lo que puede ayudar a mantenerse actualizado y alineado con las tendencias y avances en seguridad

6. **Conciencia de seguridad:** Seguir los estándares del CERT fomenta una cultura de conciencia y responsabilidad en seguridad informática dentro de la organización, lo que puede llevar a una mayor protección de los activos digitales.

En general, seguir los estándares de codificación segura del CERT puede ser beneficioso para mejorar la seguridad de los sistemas, pero también acarrera una series de desventajas específicas

Desventajas

1. **Rigidez:** Algunas organizaciones pueden encontrar que seguir todas las recomendaciones del CERT puede resultar en un código más complejo y menos flexible.

2. **Costo y tiempo:** Implementar todas las medidas de seguridad recomendadas por el CERT puede requerir una inversión significativa en tiempo y recursos.

3. **Posible obsolescencia:** Los estándares y directrices de seguridad pueden volverse obsoletos con el tiempo, lo que puede requerir actualizaciones frecuentes en el código.
4. **Adaptabilidad a contextos específicos:** Algunas recomendaciones del CERT pueden no ser directamente aplicables a todos los contextos o tecnologías, lo que podría requerir adaptaciones o personalizaciones para cada caso particular.
5. **.Complejidad adicional:** Implementar todas las medidas de seguridad recomendadas por el CERT puede aumentar la complejidad del desarrollo y mantener un equilibrio entre la seguridad y la funcionalidad de las aplicaciones.

En resumen, seguir los estándares de codificación segura del CERT puede proporcionar numerosos beneficios en términos de seguridad y calidad del código, pero es importante evaluar cuidadosamente las necesidades y capacidades de la organización para determinar la mejor manera de implementar estas medidas de forma efectiva.

Conclusiones

Las empresas no solo necesitan tener un CERT trabajando para ellos,necesitan tener uno que cumpla con todas las normas y estándares pues los dueños son las máximas responsables de evitar ataques.Por lo que después del estudio sobre este tema podemos arriba a las siguientes conclusiones:

- Los CERT para seguir buenas prácticas aplican diferentes normas y estándaras como son los FIRST,NIST e ISO
- Los CERT surgieron para evitar y dar respuesta a los ataques informáticos aunque cada día ocurran más, sin estos serían mucho más graves y frecuentes
- Están presente en todos las etapas del desarrollo de software desde la planificación hasta el despliegue y mantenimiento.
- Ofrece medidas de seguridad lo cual obviamente son ventajas, pero cuenta con un pequeño número de desventajas por lo que hay que tene ciudado y conimiento a la hora de implementarlos.

Bibliografía referenciada

- Cyber Zaintza <<FIRST – Forum of Incident Response Teams | Cyberzaintza>> 2022.
- Wilbur L. Ross<<Riks Managament Framework for Information Systems and Organizations>> diciembre de 2018.

Bibliografía Consultada

- Cyber Zaintza <<Equipo de respuesta ante incidentes>> 2022.
- DUVAN ESTEBAN URREGO FERNANDEZ<<DISEÑO DE LA DOCUMENTACIÓN TÉCNICA PARA LA IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS (CSIRT) PARA LA EMPRESA CASO DE ESTUDIO CIBERSECURITY DE COLOMBIA LTDA>>.UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA BOGOTÁ,2020
- ISO <<ISO/IEC 27001 Information security management systems — Requirements>>2023
- MANRS<<¿Cómo pueden los equipos de respuesta a incidentes de seguridad informática mejorar la seguridad del enrutamiento global?>> MANRS.org, 2023.
- National Institute of Standards and Technology. (2018). Computer Security Incident Handling Guide.
- Robachevsky Leslie Daigle, Andrei<<La iniciativa MANRS alcanza cotas más altas>>2-11-2023
- Sommer, P. L., & Brown, T. J. (2018). The state of cybersecurity incident response. Computers & Security, 78, 184-206.
- Solutions GlobalSuite<<¿Qué es la norma ISO 27001 y para qué sirve?>>20-3-2023.