ADOPCIÓN DE TECNOLOGÍAS Y BUENAS PRACTICAS DESDE UNA PERSPECTIVA DE CIBERSEGURIDAD

Adoption Of Technologies And Good Practices From A Cybersafety Perspective

Samuel Oswaldo Gaitán Bohórquez
sogaitan@ucundinamarca.edu.co
samuel.ogb@gmail.com

Universidad de Cundinamarca, Facultad de Ingeniería, Programa [Ingeniería Electrónica]
Alcaldía de Fusagasugá, Oficina TIC, pasantía [ciberseguridad]

Resumen
La ciberseguridad no es una palabra de moda, sino que se ha incorporado a los reglamentos y marcos de trabajo. Tenga en cuenta que la ciberseguridad se centra en las amenazas basadas en Internet que atacan los datos digitales y los equipos de TI. Para las organizaciones, un inventario de dispositivos es el primer paso para implementar los controles de seguridad críticos, lo que se puede lograr utilizando herramientas como el agente Fusion-Inventory de GLPI.
La mejor manera de prevenir ataques consiste en mejorar el conocimiento y la concientización, de esta manera se puede adquirir experiencia práctica mediante la aplicación de los principios de ciberseguridad para proteger datos de valor para los usuarios y para la entidad. Estas habilidades mejoradas son aplicables en el lugar de trabajo. Comprender las amenazas de la ciberseguridad ayuda a detectarlas, convirtiéndolas en un sensor valioso para la entidad y no simplemente en una vulnerabilidad.

Palabras Clave: GLPI: Aplicación web para gestión de sistemas de información; Ciberseguridad: es el área de la informática encargada de la protección de la infraestructura de red y todo lo vinculado con la misma; Vulnerabilidad: situación que permite el robo o destrucción de información, también puede alterar o detener el funcionamiento de los diferentes dispositivos.

Abstract
Cybersecurity is no longer a buzzword but has been incorporated into regulations and frameworks. Keep in mind that cybersecurity focuses on Internet-based threats that attack digital data. For organizations, a device inventory is the first step in implementing critical security controls, which can be accomplished using tools such as GLPI's Fusion-Inventory agent.
The best way to prevent attacks is to improve knowledge and awareness, in this way practical experience can be gained by applying cybersecurity principles to protect valuable data for users and for the entity. These enhanced skills are applicable in the workplace. Understanding cybersecurity threats helps to detect them, making them a valuable sensor for the entity and not simply a vulnerability.

Keywords: GLPI: Web application for information systems management; Cybersecurity: it is the IT area in charge of protecting the network infrastructure and everything related to it; Vulnerability: situation that allows the theft or destruction of information, it can also alter or stop the operation of the different devices.

1. INTRODUCCIÓN

La Ciberseguridad es la práctica de defender de ataques maliciosos a los ordenadores, servidores, dispositivos móviles, los sistemas electrónicos, las redes y los datos. (según Kaspersky) [1]

Algunas de las amenazas más comunes son:

- Virus: un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- Troyanos: un tipo de malware que se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos.
- Spyware: un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.
- Ransomware: malware que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
- Adware: software de publicidad que puede utilizarse para difundir malware.
- Botnets: redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en

línea sin el permiso del usuario.

El conocimiento de estas amenazas permite tomar medidas preventivas, de corrección y de recuperación.

El concepto se aplica también como protección o seguridad: en redes, en las aplicaciones, en la información, en la seguridad operativa, en la recuperación frente a ataques y la continuidad de las operaciones normales y finalmente en la capacitación del usuario. Los correos electrónicos maliciosos, la ingeniería social y los sofisticados intentos de fraude cibernético son ahora la norma. A medida que transcurre el tiempo la Ciberseguridad ha sido un tema muy importante. Su importancia se elevó por el aumento de ciberataques en todo el mundo y del rol que cumple en la seguridad tecnológica. Las organizaciones están lidiando con la forma de mejorar su postura general de seguridad de la información, y deben darse cuenta de que esto comienza con el conocimiento y la conciencia a todos los niveles. [2]

2. MEDIDAS DE CIBERSEGURIDAD

En el caso en que sea atacada la entidad, existen unas medidas o pasos que debe seguir el oficial o equipo de seguridad, a continuación, se detalla las medidas para respectivo procedimiento.

ANÁLISIS

El análisis es el primer paso para detectar un ataque. En esta fase se buscará la naturaleza de la información, la extensión del daño, las posibles intenciones del intruso, las herramientas que puede utilizar y las vulnerabilidades utilizadas. Toda esta información es fundamental para identificar las señales que permitan reconocer y generar la alerta correspondiente. Al considerar un conjunto más amplio de eventos, es posible identificar alertas para nuevos riesgos, como nuevos métodos de ataque.

ALERTA

En un mundo de mensajería casi instantánea, unos minutos pueden significar la diferencia entre una interrupción severa y un evento manejable. Para distribuir la información disponible en el paso anterior a tiempo, se necesita una infraestructura segura para proporcionar una comunicación confiable entre los propietarios de la infraestructura crítica, los operadores y los proveedores de servicios.

RESPUESTA Y RECUPERACIÓN

Una vez emitida la alerta, el gobierno debe respaldar la gestión de crisis para responder a las amenazas y ataques a los sistemas de información críticos de la entidad, el gobierno autónomo, el sector público y el sector privado a pedido.

No existe ninguna tecnología que pueda hacer que la red sea completamente segura. Una forma de reducir las pérdidas asociadas con los ataques cibernéticos es desarrollar planes de contingencia adecuados y probados. Además, se deben establecer planes de asistencia mutua entre los diferentes componentes de la infraestructura clave para reducir los efectos en cascada causados por las relaciones mutuas. Todos estos planes deben llevarse a cabo bajo la coordinación de un oficial de seguridad encargado, que debe reportar directamente a la agencia gubernamental responsable de la seguridad del ciberespacio, o las autoridades designadas. Deberían utilizarse ejercicios de simulación para probar la eficacia de los planes de seguridad y emergencia. De esta manera, es posible evaluar el impacto potencial del ataque y la capacidad de las partes públicas y privadas para coordinar la gestión, respuesta y recuperación de incidentes.

INTERCAMBIO DE INFORMACIÓN

Compartir la información del incidente es fundamental. Existen dificultades para lograr este objetivo, como el temor a que los datos privados o potencialmente comprometidos puedan llegar al dominio público si se comparten secretos con el gobierno. Las preocupaciones sobre la ventaja competitiva pueden impedir el intercambio de información entre empresas del mismo sector. Prueba de ello es que la mayoría de los delitos cibernéticos los llevan a cabo internamente las propias organizaciones afectadas, y estas organizaciones realizan investigaciones secretas. Los resultados casi nunca se hacen públicos.

REDUCCIÓN Y CORRECCIÓN DE VULNERABILIDADES DE SOFTWARE

Todos los días aparecen nuevas vulnerabilidades de software. La corrección la proporciona normalmente el fabricante a través de un "parche". Sin embargo, muchos errores conocidos (hay errores arreglados) persistirán en el sistema durante mucho tiempo. El software no corregido en la infraestructura crítica los hace vulnerables porque estos defectos se pueden usar para controlarlos.
La difusión de información sobre la existencia de estas vulnerabilidades y cómo corregirlas es fundamental, pero esto plantea un problema, ya que su difusión pública no solo ayuda a desarrollar medidas correctivas, sino que también crea oportunidades para los atacantes. Para solucionar este problema, debe existir un canal seguro para transmitir esta información. Un enfoque puede ser la red de centros de análisis e intercambio de información antes mencionada. [3]

PRINCIPIOS

es importante tener en cuenta los principios básicos de la seguridad de la información, conocidos por las iniciales CIA [en inglés]:

- Confidencialidad:

Mantenga la información y los sistemas seguros contra el acceso no autorizado (incluyendo la "piratería informática"). Mantenga los datos seguros, evite que las cuentas de correo electrónico se vean comprometidas.

- Integridad:

Evite que se manipulen los datos. Evite que un delincuente envíe mensajes de correo electrónico desde una cuenta comprometida, como si se hiciera pasar por el propietario. Impida que un delincuente manipule los saldos de las cuentas o los datos comerciales.

- Disponibilidad:

Garantice que los datos y los sistemas sigan siendo accesibles. Ransomware, huracanes y otros desastres podrían afectar la capacidad de continuar con las operaciones comerciales. [4]

3. GLPI

GLPI es una aplicación para la gestión de servicios de TI. El agente FusionInventory (FIA) envía la descripción de los equipos Windows a FusionInventory de GLPI (FI4G) como parte de la información de inventario. Además, permite obtener la hoja de vida de los diferentes equipos, incluidos los servidores.
identifica la condición de cada equipo de TI de la entidad en tiempo real con el inventario multiplataforma automático incorporado en GLPI. Detecta con anticipación renovaciones o actualizaciones de software o hardware a ser ejecutados. [5]

4. CONCLUSIONES

- El conocimiento de técnicas de seguridad informática puede ser tan valioso como la información que se protege, la infraestructura y los equipos.
- Estar actualizado en temas de ciberseguridad no es cuestión de lujo o estatus, es una necesidad de estar preparados para la creciente creatividad en los ataques, y el aumento de las amenazas.
- Todo sistema es vulnerable en cierta medida, por ello es indispensable la aplicación de los principios de ciberseguridad.
- La aplicación de herramientas como GLPI facilita o automatiza tareas periódicas como son mantenimientos, actualizaciones e inventarios.

REFERENCIAS

[1] Kaspersky, «Kaspersky,» 25 Mayo 2020. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

[2] Iniseg, «La importancia de la Ciberseguridad y sus profesionales,» 16 julio 2020. [En línea]. Available: https://www.iniseg.es/blog/ciberseguridad/la-importancia-de-la-ciberseguridad-y-sus-profesionales/.

[3] J. P. Maroto, «EL CIBERESPIONAJE Y LA CIBERSEGURIDAD,» 2009. [En línea]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=4549946.

[4] R. Mejia, «Smatekh,» [En línea]. Available: https://blog.smartekh.com/que-es-la-triada-de-seguridad-o-cia-triad-y-por-que-deberia-interesarte.

[5] GLPI, «GLPI,» 2021. [En línea]. Available: https://glpi-project.org/es/.