SEGURIDAD EN PROFUNDIDAD
"Los pro y los contra"

Bernal Garnica, Miguel Alberto
Universidad Piloto de Colombina
Bogotá, Colombia
miguel.bernal@gmail.com

Abstract- This document aims to make an analysis of the pros and cons of the enforcement of a security system in depth in a company or organization, starting with its definition, relevant aspects to consider in creating a draft reaching this size and show the importance and benefits can be obtained for a company implementing a security project.

Resumen- En el presente documento se pretende realizar un análisis sobre los pro y los contra que tiene la aplicación de un sistema de seguridad en profundidad en una empresa o entidad, comenzando por su definición, aspectos relevantes a tener en cuenta en la creación de un proyecto de esta magnitud y llegando a mostrar la importancia y beneficios que se puede obtener una empresa en la aplicación de un proyecto de seguridad.

Índice de términos- Hardware, software, penetración, integridad, disponibilidad, confidencialidad, tripwire, backup, intruso, vulnerabilidad, hardening.

I. INTRODUCCIÓN

¿Seguridad en profundidad? ¿Sabemos en qué consiste? ¿Cómo aplicarla? ¿Si existen pros y contras en su aplicación? Algunas de las definiciones que verán a continuación nos permitirán abrir la puerta a esta compleja pero definitivamente herramienta esencial en el manejo de información, la cual debe aplicarse como una de las buenas practicas que exige el dinamismo del mundo de hoy. Se pueden encontrar definiciones como *"el concepto de protección de una red de ordenadores con una serie de mecanismos de defensa organizados de tal manera que, si uno de ellos falla, otro está disponible para tomar su lugar"*[1]. *"Se trata de un modelo que pretende aplicar controles en seguridad para proteger los datos en diferentes capas"* [2]. "*En sus inicios se refirió a una estrategia militar que tiene por objetivo hacer que el atacante pierda el empuje inicial y se vea detenido en sus intentos al requerirle superar varias barreras en lugar de una*"[3]. Esta estrategia o sistema es de origen militar, y data de las estrategias militares y las diversas adecuaciones de las ciudades para convertirlas en fortines militares o los mecanismos que utilizaban los militares para planear sus defensas y batallas, en este documento se pretende destacar los beneficios y contras de colocar una solución de seguridad en una entidad o organización.

II. SEGURIDAD EN PROFUNDIDAD

Se debe aclarar que todo lo relacionado con seguridad comienza en las estrategias militares que se aplicaban en las guerras y que después se pasa al terreno industria y en la actualidad está incursionando a los sistemas de información.

En síntesis podríamos decir que Seguridad en profundidad es una herramienta que podemos aplicar no solo en sistemas sino en cualquier momento, en cualquier lugar, en la vida diaria, en el trabajo, etc., el concepto general podría ser: la seguridad en profundidad es utilizar diversas barreras para evitar el ingreso a…, y su uso no es para evitar que ocurran intrusiones o accesos no permitidos por terceros o personal no autorizado, se plantea en las estrategias que estén planteadas para dificultar el ingreso u otras acciones que favorezcan el riesgo del sistema y de la información almacenada. Para lo cual se ajustan tantas defensas como sean posibles y de esta manera podemos lograr que el atacante o intruso desista en el vulnerar el sistema de los dispositivos o el desear apropiarse de información de interés privado, de connotación propiamente profesional.

Hablar de seguridad en profundidad implica conocer a detalladamente, los aspectos más relevantes de la entidad que se pretende asegurar y para esto es indispensable responder algunas preguntas que permitirían establecer el diagnostico de esta, con el fin de dar un acertado camino a seguir, estas pueden ser:

- ¿Cuál es la razón de ser de la empresa? *Misión, Visión, objetivos, objeto de la empresa, tipo de empresa, número de empleados, tipo de información que manejan, etc.*
- ¿Qué es lo que se quiere asegurar?
- ¿De qué y de quien se quiere asegurar?
- ¿Con que presupuesto se cuenta?
- ¿Hasta dónde se quiere asegurar?

Una vez se conozca a la empresa y teniendo en cuenta con que presupuesto cuenta la entidad para llevar acabo la estrategia de seguridad en profundidad que se vaya a implementar, se deben definir claramente los siguientes aspectos que favorecerían la ruta más pertinente a recorrer:

- Lo que se quiere asegurar. (la Información, el hardware o el software): es importante tener claro a qué le vamos a aplicar seguridad en profundidad ya que para cualquiera de las tres partes es un proyecto diferente y se utilizarían herramientas diversas.

- ¿Qué se quiere evitar que ataquen? (integridad, Disponibilidad, confidencialidad, el no repudio, la autenticidad): es muy importante establecer que es lo que se quiere evitar que ocurra, para poder realizar un levantamiento de información completo y realizar una planeación específica de la tecnología o software que utilizaremos en el proyecto de seguridad.

- ¿Cómo se quiere evitar? Una vez definido lo que se quiere asegurar se procede a revisar que existe en el medio tecnológico y que brinde de protección que se requiere.

- ¿Tipo de tecnología que se utilizara? Para esto es importante tener en cuenta el presupuesto y lo que se quiere evitar que ataquen, ya que podemos utilizar software free o herramientas propietarias que podrían superar las expectativas que se tiene en el proyecto.

- ¿Qué tipo de monitoreo se implementara? Este punto es de gran importancia ya que se puede llegar a implementar el sistema de seguridad más robusto y costoso que exista en el mercado y que realice de todo con las

herramientas más sofisticadas existentes, pero si no se tiene una herramienta que nos permita mirar su funcionamiento y nos ayude a detectar falencias de seguridad o por lo menos nos informe que algo raro está pasando no sirve de nada, ya que tener cajas negras sin ninguna funcionalidad de monitoreo es colocar barreras que nunca se vigilan y no permite saber que está sucediendo.

- ¿Qué personal se requiere?, es importante definir el tipo de personal que se necesita para realizar el proyecto de seguridad, esto requiere de personal técnico, profesional y especializado que se necesite para realizar las diversas actividades del proyecto de seguridad.

Los pilares a tener en cuenta en seguridad son:

Prevención: *"Preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo"* [4], "*Utilizando métodos de autenticación, identificación, control de acceso, transmisión segura, plataformas heterogéneas, sistemas honeyport, etc."* [5].

Detección: "*Acción y efecto de detectar"* [6], "*A través de programas de auditoria como Tripwire o Nagios, encargados de realizar chequeos de integridad, proveer y presentar información al instante sobre el estado actual del sistema"* [7].

Respuesta: "efecto que se pretende conseguir con una acción" [8]. "*Implementando métodos de backup y software de análisis forense (para detectar que hizo el intruso y que vulnerabilidad explotó)"* [9].

Figura 1. Mecanismos de Seguridad

En la gráfica se puede observar que la seguridad esta sostenida en tres factores prevenir, detectar y responder que son el ciclo que siempre se debe tener en cuenta para realizar un proyecto de seguridad.

Una vez aclarado los aspectos anteriores, se debe iniciar el proyecto de seguridad donde se defina un objetivo general y varios objetivos específicos que definan el alcance del proyecto de seguridad, esto quiere decir donde inicia y donde termina el proyecto que se pretende realizar. Se debe realizar una concientización al personal de la entidad y dejar muy claro que un proyecto de seguridad implica involucrar a todos los funcionarios y a los diferentes actores de la entidad, esto significa que se debe comprometer desde aquellos que son las cabezas visibles de la empresa hasta el personal de servicios de apoyo general de la entidad incluyendo agentes externos que tienen que ver con la entidad, todos deben debe estar en pro del proyecto de seguridad, colaborar y poner en práctica las diferentes políticas que se implementen en la empresa.

Si no se logra que la gerencia asuma su rol en el proyecto de seguridad, es un indicador claro que el proyecto no cumplirá con los objetivos ni el alcance lo se halla definido, ya que es primordial que todos deben estar comprometidos para el cumplimiento de los objetivos de la organización para con este particular, lo que conlleva a la necesidad de conocer el proyecto, mantenerse Informados, conscientes y dispuestos para asumir

compromisos y los cambios que el proyecto de seguridad requiera y que se implementara.

Superado los temas anteriores y definidos los objetivos y el alcance del proyecto se procede a realizar el análisis necesario que nos permitirá ver la necesidad real de lo que se requiere asegurar y buscar que herramientas de hardware y software permitirá realizar la implementación del proyecto de seguridad.

En el mercado actual y observando el continuo crecimiento de la tecnología en materia de seguridad, se puede encontrar muchas herramientas que permiten alcanzar los objetivos trazados en el proyecto o que se pueden adaptar a las necesidades requeridas para la organización, también puede ocurrir que solamente se necesite realizar endurecimiento de servidores (hardening) y software especializado (firewall, IPS, etc.) que cumplan con las especificaciones de seguridad que se requieren para la entidad.

Hablar de seguridad en profundidad no significa tener la última generación de herramientas de seguridad del mercado, ni tampoco significa tener los ingenieros más expertos del mercado en herramientas, que en diversas ocasiones no son necesarios para lograr el alcance trazado para la entidad.

Hablar de seguridad en profundidad significa como se mencionó anteriormente dificultar el ingreso y que sea lo más complejo posible el ingreso a los sistemas de información de la entidad, para que los terceros desistan del intento y evitar así accesos no permitidos, para llegar a una conclusión podemos destacar ejemplos de la vida diaria los cuales pueden llegar a ser aplicables en la seguridad de los sistemas información sin dejar atrás que los inicios de la seguridad en profundidad, se debe a las tácticas militares utilizadas en las grandes batallas, que permitían perder o ganar una batalla según la estrategia utilizada en su momento. Llevando esto al día a día en una entidad, son as batallas diarias que se tienen que emprender para evitar que sean vulnerados los sistemas de vigilancia instalados, los sistemas de información, las páginas web, aplicativos, las contraseñas, los accesos a aplicativos etc, hablar de seguridad en profundidad es colocar, instalar y configurar diferentes tipos de barreras ya sean equipos especializados o software solas o en conjunto para evitar intrusiones o accesos no autorizados en los sistemas información.

Hablar de seguridad en profundidad implica tener claros algunos antecedentes:

- Conocer la historia de las vulnerabilidades y ataques que han ocurrido, estar actualizado en los nuevos casos para observar el modus operandi de los diversos hacker, cracker, etc. que existen alrededor del mundo.

- Conocer la terminología que se utiliza en el mercado y sobre todo en las páginas web que existen para este tipo de intrusiones y ataques (Vulnerabilidades, exploit, ataque, pentest, etc).

- A partir del conocimiento aplicar los métodos o las buenas prácticas que existen para poder protegerse o defenderse, y sobre todo recuperarse ante estos eventos.

- Conocer las herramientas de software y hardware que existen en el marcado. (Tanto libres como pagas).
- Estar vinculado a eventos, paginas, empresas de seguridad que permitirá estar actualizados sobre los últimos métodos de utilizados por terceros para vulnerar sistemas.

- Identificar las posibles vulnerabilidades de la organización a la que pertenece y tomar mecanismos de prevención para estos eventos.

- Concientizar al personal de la organización de la importancia que tiene la seguridad y los métodos que se utilizar para obtener información vital de la empresa.

- Conocer de redes, comunicaciones, sistemas operativos, herramientas de seguridad, hardening, etc, que realmente son las posibles vulnerabilidades que terceros o intrusos pueden utilizar para realizar ingresos no permitidos a la entidad.

- Trabajar en conjunto con las diferentes áreas de la empresa pero sobretodo del área de tecnología para definición de estrategias y posterior aplicación de las mismas.

III. CONTRAS DE LA SEGURIDAD EN PROFUNDIDAD

Siguiendo con el tema se pasa ahora abordar los pros y los contras que tiene la defensa en profundidad para dar a conocer los beneficios y problemáticas de este proyecto.

En relación a los contras los de mayor relevancia pueden ser:

- Según el tamaño de la entidad, tener una buena defensa en profundidad implica tener amplio presupuesto, para invertir en herramientas sofisticadas con lo cual se protege, analiza, anticipa, correlaciona eventos y se da posibles soluciones al diverso mundo de problemáticas o vulnerabilidades que son encontradas diariamente en el área de las TIC.

- Implica también costos de contratos y capacitación de los ingenieros en herramientas especializadas del mercado y en su gran mayoría tienen un grado de complejidad alto y que no son fáciles de manejar y administrar, aclarando que en su mayoría no son intuitivas, además que necesitan un alto grado de conocimiento en redes, comunicaciones, seguridad, sistemas operativos, etc., el grado de complejidad de estas herramientas hace que se gaste mucho tiempo en aprender a manejarlas y en muchas ocasiones que se tenga que capacitar a los administradores de la entidad para poder colocarlas en funcionamiento. todo esto y sumado a la diversidad de hardware y software especializado que sale al mercado frecuentemente hace que en ocasiones sea complejo la definición de escoger la herramienta o herramientas apropiadas para la entidad.

- Podría aseverar que están completo el tema que no solo basta con capacitar o contratar a un ingeniero sino que hay que capacitar y/o contratar un pool de ingenieros especializados en cada herramienta para llegar a tener un mediano o buen esquema de seguridad para la organización.

- La sobre carga laborar para los ingenieros que administran los sistemas de información y de seguridad de la empresa es grande, ya que generalmente los responsables de administrar los centros de datos y comunicaciones son unos pocos, Generalmente lo que realiza una entidad es sumarle a las diversas tareas de administración el compromiso de implementar y administrar los sistemas de seguridad esto con lleva a que en un grupo de personas se vuelvan indispensables y a la

vez una de las mayores vulnerabilidades de la entidad por su alto grado de conocimiento de la infraestructura tecnológica de la empresa.

- Hablar de que existen herramientas libres con las que se puedan llegar a tener un nivel aceptable de seguridad en profundidad no quiere decir que esté protegido ya que lo barato no siempre es lo mejor y las herramientas libres no siempre son las más seguras o completas ya que los programadores o las empresas que diseñan estos sistemas pueden dejan en su interior huecos ocultos para poder ingresar y así poder vulnerar las organizaciones.

- Hablar de defensa en profundidad siempre es incompleto ya que los problemas o los huecos de seguridad que se encuentran a diario son altos en las organizaciones, se puede destacar que los usuarios al interior de la organización es el mayor problema ya que no respetan ni cumplen las policías establecidas de seguridad para la organización, ya que en su mayoría solo cumplen con un trabajo y lo demás no les importa y lo dejan de lado.

- El tener que cambiar frecuentemente las contraseñas y sumado a que los requerimientos de complejidad de los password cada vez son mayores es un trauma que no pueden aceptar y sobretodo asimilar, todas estas políticas son enviados a la basura o nunca son puestos en práctica ya que encontramos en las organizaciones claves en papelitos, las claves personales las conocen varios funcionarios, los usuarios son prestados por los privilegios que tienen, dar acceso a personal ajeno a la entidad, llevar la información para el hogar, en fin muchos casos que no son bien tratados y analizados y que en ultimas a pesar que se tenga la infraestructura más robusta, las mejores políticas redactadas, capacitaciones frecuentes, etc., Esto quiere decir que es la vulnerabilidad más común y de las más difíciles de solucionar ya que la información que manipulan los usuarios puede ser tan importante como la empresa lo requiera.

- Otro problema de gran envergadura al hablar de seguridad en profundidad es el de reconocer que la tecnología está en constante cambio y cada día a día sale algo nuevo y que con relación a seguridad falta mucho tiempo para colocarla a punto y no se ha terminado de inventar. Asumir la premisa que en la teoría todo es fácil y aplicable no es tan cierto ya que la vida diaria es compleja, reunir y unificar todos los criterios de seguridad que se deben aplicar es complicado y dispenioso.

- Por esta razón dejo en el tintero las siguientes inquietudes:

  - ✓ ¿Realmente existe seguridad en profundidad en algún lugar de este planeta?.
  - ✓ ¿La humanidad está preparada para asumir los retos de la seguridad en profundidad?
  - ✓ ¿Los altos costos del software y hardware ayudan a implementar sistemas de seguridad en profundidad?
  - ✓ ¿Si es bueno tener herramientas Free?, etc.

IV. PROS DE LA SEGURIDAD EN PROFUNDIDAD

Para cerrar el tema se analizara ahora los pro que tiene la seguridad en profundidad ya que esta nos permite mejorar y no quiero decir con esto que se eliminan los problemas de seguridad ya que no existe en el mercado ninguna herramienta que realice todas las labores de seguridad que se requieren para tener un sistema de seguridad en profundidad aplicado y funcionando. Pero es una de las buenas prácticas que debe aplicar en las entidades.

Un sistema de seguridad en profundidad nos permite:

- Hardening de los equipos periféricos, servidores y telecomunicaciones que utilizamos: realizar aseguramiento de las herramientas y equipos que se tienen a disposición como lo son equipos de comunicaciones, herramientas de seguridad, servidores, etc., es de vital importancia, ya que esto permite configurar solamente lo que se necesita dejar abierto al público, y a la empresa, generalmente esta buena práctica de asegurar los equipos y periféricos no se tiene en cuenta o no se realiza dejando a disposición de terceros puertos y protocolos abiertos que pueden ser utilizados por terceros para realizar penetraciones o intrusiones a los sistemas que administramos dejando a disposición de terceros la información de la entidad o permitiendo que utilicen los sistemas que administramos para que sean utilizados para otros fines sin que nos demos por enterados.

- Para un administrador es importante tener claro con que herramientas cuenta, que tan efectiva puede ser y que beneficio se puede obtener, además de tener un check list de lo que necesita y como lo va a utilizar para evitar perdida de información o que los recursos informáticos sean utilizados con fines diferentes y que se vea involucrado eventos incontrolables y que pueden perjudicar a la entidad.

- Accesos restringidos y con prioridades definidas: Conocer las herramientas con las que se cuenta es importante, pero el acceso a las herramientas y recursos es de mayor importancia, ya que realizar una verificación de los usuarios, pero sobretodo los permisos que estos deben tener sobre la plataforma, ya que otorgar más permisos de los que se necesitan puede llevar o acarrear diversos problemas que en muchas ocasiones no son fáciles de solucionar.

- Tener definidos los roles y permisos de los usuarios ayudara a mantener un estricto control de los recursos y permitirá establecer unas mejores políticas de uso y de seguridad para la entidad. Un usuario con demasiados permisos y privilegios puede ser abordado por terceros que pueden aprovechar esto para adquirir información que solo debe conocer la entidad o incluso robar la información para entregarla a la competencia y llevar a quiebra la entidad.

- Monitoreo de los diferentes sistemas: tan importante como tener las herramientas que compliquen el ingreso a los sistemas es tener un sistema de monitoreo que permita saber antes que es lo que está pasando con los sistemas que administramos, para un administrador saber primero los eventos que están ocurriendo es vital ya que se puede evitar o por lo menos separar o aislar lo que

no se quiera que ocurra en el sistemas que se administran.

No solamente permite conocer de primera mano lo que sucede sino que nos facilita desplegar procesos correctivos o preventivos cuando se comprueba que las herramientas mayor aumento de los recursos tecnológicos, programar la adquisición de nuevos recursos tecnológicos, etc. En fin monitorear los sistemas permite conocer los recursos con los que se cuenta, como se está utilizando, tecnológicas se están quedando sin recursos, están siendo muy utilizadas, las fechas de que se requiere, programar actualizaciones, mantenimientos, adquisición de nuevas herramientas, etc.

Para un administrador monitorear es una de las tarea más importantes ya que es la herramienta que permite conocer las posibles intrusiones y de esta forma actuar ante cualquier eventualidad.

- Conocer primero que es lo que está sucediendo en los equipos, la red, servidores, aplicativos, etc, es importante ya que esto permite tomar medidas de precaución para evitar que la intrusión sea mayor, ya sea solucionando el problema, o aislando los servicios o servidores o equipos de comunicaciones o por ultimo bajando los sistemas para evitar que sigan sacando provecho de las vulnerabilidades que explotaron.

- Algo que se puede destacar de la seguridad en profundidad es que se puede colocar zonas de fácil acceso o señuelos para que intrusos ingresen y se puede detectar que es lo que hacen y como lo hacen.

- Uno de los grandes compromisos y que deja mucho para el crecimiento personal de los ingenieros es el tener que estarce actualizando día a día en las herramientas que se manejan, en las últimas vulnerabilidades que encuentran, estar realizando pruebas de penetración para verificar si el sistema de seguridad está funcionando.

En fin hablar de seguridad en profundidad es amplio e interesante para las personas que ingresan en este mundo y se apasionan por estos procesos, ya que el aprendizaje es permanente y continuo, el interés nunca se puede perder ya que cada día hay algo que mirar, corregir o monitorear, ingresar en este mundo de la seguridad es tan atractivo que cada día se busca buscar mejorar lo que se tiene o implementar nuevas herramientas o mecanismos de seguridad, llegar a aplicarla seguridad en profundidad es tan seductor que no permite dejar de investigar, analizar, proponer, definir y de buscar las mejores prácticas para colocarlas en producción y verificar si son funcionales o no y tener satisfacción del deber cumplido.

V. CONCLUSIONES

La seguridad en profundidad no impide que los sistemas sean vulnerados por terceros.

La seguridad en profundidad pretende implementar y aplicar un sistema de buenas prácticas en pro de la organización.

Ingresar al mundo de la seguridad en profundidad implica mantenerse actualizado en los diferentes campos que integra un proyecto de esta magnitud. (Redes, servidores, seguridad, comunicaciones, etc.).

El proyecto de seguridad debe involucrar a todo el personal de la organización, desde el más alto cargo gerencial de la entidad, hasta el funcionario

con el cargo más bajo, si esto no ocurre el proyecto se caerá de su peso y no funcionara.

No Sirve tener el sistema de seguridad en profundidad más robusto, con las mejores políticas, procesos y procedimientos establecidos sino se cumple con dar a conocerla y capacitar al personal en la utilización de la misma.

REFERENCIAS

[1] Sastry A. (2012, Noviembre). Arquitecto de seguridad sénior de Savvis. [Online] Available; http://searchdatacenter.techtarget.com/es/consejo/Como-planificar-una-red-segura-mediante-la-practica-de-la-defensa-en-profundidad

[2] Bortnik, S. (2010, Mayo 24). Analista de seguridad. [Online] Available; http://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

[3] Sentineldr. (2010, Noviembre 5). Noticias sobre seguridad de la información. [Online] Available; http://blog.segu-info.com.ar/2010/11/defensa-en-profundidad.html

[4] Real academia española. (2014) Edición 23. [Online] Available; http://lema.rae.es/drae/

[5] Sarubbi, J. (2008). Técnicas de defensa: Mecanismos comunes bajo variantes del sistema operativo Unix. [Online] Available; https://books.google.com.co/books?id=o3war7zF-g8C&pg=PA6&lpg=PA6&dq=seguridad+en+profundidad+en+sistemas&source=bl&ots=7_WWPgISuX&sig=K-6zRQdJgsu3C1sPRZ--gTavUs4&hl=es&sa=X&ei=wIw-Vd_sDqrIsATTzIGwDw&redir_esc=y#v=onepage&q=seguridad%20en%20profundidad%20en%20sistemas&f=false

[6] op cit.

[7] Sarubbi, J. (2008). Técnicas de defensa: Mecanismos comunes bajo variantes del sistema operativo Unix. [Online] Available; https://books.google.com.co/books?id=o3war7zF-g8C&pg=PA6&lpg=PA6&dq=seguridad+en+profundidad+en+sistemas&source=bl&ots=7_WWPgISuX&sig=K-6zRQdJgsu3C1sPRZ--gTavUs4&hl=es&sa=X&ei=wIw-Vd_sDqrIsATTzIGwDw&redir_esc=y#v=onepage&q=seguridad%20en%20profundidad%20en%20sistemas&f=false

[8] Real academia española. (2014) Edición 23. [Online] Available; http://lema.rae.es/drae/

[9] op cit.

FIGURAS

[1] Sarubbi, J. (2008). Técnicas de defensa: Mecanismos comunes bajo variantes del sistema operativo Unix. [Online] Available; https://books.google.com.co/books?id=o3war7zF-g8C&pg=PA6&lpg=PA6&dq=seguridad+en+profundidad+en+sistemas&source=bl&ots=7_WWPgISuX&sig=K-6zRQdJgsu3C1sPRZ--gTavUs4&hl=es&sa=X&ei=wIw-Vd_sDqrIsATTzIGwDw&redir_esc=y#v=onepage&q=seguridad%20en%20profundidad%20en%20sistemas&f=false