UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

PRUEBA PRÁCTICA INGENIERÍA EN SISTEMAS

TEMA:

ANÁLISIS DE VULNERABILIDAD DE LA BASE DE DATOS EN LA EMPRESA ISANET DEL CANTON MONTALVO

EGRESADO:

BETTY SAMANTA VELOZ PEÑAHERRERA

TUTOR:

ING. HARRY SALTOS VITERI

AÑO

2021

INTRODUCCION

La información es el activo más importante de una organización y por lo tanto debe de proporcionársele los cuidados necesarios, ya que en los últimos años se han visto casos de muchas vulneraciones e inseguridades sufridas en empresas importantes, esto ha hecho que además se ponga mucho interés en la seguridad de la información sobre todo de las organizaciones y hogares que están conectados a internet pues es el medio principal por el cual se pueden vulnerar.

Las empresas que brindan servicio de internet deben además ser el primer nivel de seguridad Con qué cuentan los clientes que se conectan a la red a través de ellos sin embargo estos tienen muchas deficiencias sobre todo en los territorios donde existen varios proveedores con equipos tecnológicos que simplemente sirven para distribuir la red, pero no para hacer filtrado, pues eso además les demanda un poco más de tiempo y un posible retraso en su calidad de servicio.

El dar Seguridad a las bases de datos en las empresas de internet Cómo es el caso de ISANET, Qué cuenta con información importante en su base de datos, esto es, registro de clientes y sus deudas, así como los pagos realizados Direcciones IP Mac y demás información importante relacionada con el cliente con lo técnico y lo Financiero, Y resulta de Vital importancia que estaba sedado sea Bien protegida

La empresa ISANET, ha tenido durante los dos últimos años, Muchos problemas con la caída de su servicio no solamente por la conectividad una infraestructura de red que tiene sino que su base de datos con la que está conectado su sistema de conexión y desconexión es automatizadas ha incidido con esto y se ha debido a ciertas fugas de información oa pérdida de registros en varias tablas de su base de datos por lo que este

caso estudio es necesario y pertinente y de seguro permitirá alguna nueva estrategia o análisis que ayude a la prevención y correcta se seguridad de su Base de Datos. (villalobos, johonny;Vulnerabilidad de Sistemas Gestores de Bases de, 2017)

Este caso de estudio está amparado con la sublínea de investigación de la carrera de ingeniería en sistemas, es así que, su línea de investigación es la siguiente: "Comunicación y emprendimientos empresariales y tecnológicos, desarrollo de Sistemas de la información y la sublínea es procesos de datos y telecomunicaciones"; por lo tanto, el presente proyecto de investigación tiene como finalidad analizar la vulnerabilidad que existe en la base de datos de ISANET, empresa proveedora de internet ubicada en el cantón Montalvo.

DESARROLLO

La empresa ISANET Proveedora de servicios de Internet del cantón Montalvo es una de las organizaciones más grandes que brinda este servicio en la ciudad Además de que muchos hogares son conectados también desde sectores alejados de la ciudad esto es la zona rural es una empresa que cuenta con un Gerente, el Ing. Joffre Navarro, El mismo que además tiene un equipo técnico de 12 empleados, expertos en redes y comunicaciones qué, continuamente se encuentran brindando servicios de soporte y atención a los clientes, para que no existan perdidas en las conexiones y alcanzar la calidad de servicio a satisfacción.

Durante los dos últimos años la calidad de servicio se ha visto afectada, a partir de su base de datos, pues en esta, se almacenan registros de deudas financieras con los clientes y no se le ha brindado la protección requerida necesaria, teniendo muchos agujeros de seguridad abiertos esta base datos, que se vio vulnerada en muchas ocasiones, dejando sin conexión a más de 425 familias y en momentos en que los integrantes de estas tenían clases virtuales o teletrabajo; en su inicio, no lograban determinar cuál era el inconveniente de las desconexiones y se pensaba que eran cortes de fibra o alguna causa del exterior del mismo ISP

La metodología utilizada en el presente estudio de caso es cualitativa, al contar como medio de recolección de información y datos para su análisis, con técnicos que han permitido validar esta investigación con entrevistas fundamentadas en un cuestionario relacionado con la seguridad de los ISP y las Bases de Datos.

Su construcción está enfocada a los posibles factores que generarían la problemática del caso presente, soluciones y/o recomendaciones que podrían brindar una mejoraría del nivel de servicio y conectividad de ISANET.

Es así que, al realizar las preguntas relacionadas (ANEXO 1), se ha analizado lo siguiente, confrontando las opiniones de los expertos y la de la autora de este caso de estudio, así como también, con el texto de fuentes confiables del que se encuentra nutrido este trabajo de caso de estudio.

El análisis es el siguiente: la vulnerabilidad de la empresa no se vende ni se filtra, la información de los clientes es vitar y útil para ISANET, porque son datos personales y financieros, así como datos técnicos, y manteniendo asegurada las bases de datos con buenas políticas, se logra superar estos inconvenientes.

La empresa cuenta con una sola base de datos donde abarca a todos sus clientes con su respectiva información, ha esta base de datos, la seguridad que se le aplica es la de generar un tipo de protección al realizarle backups, sin embargo, estos no son automáticos, permitiendo que en algún momento pueda no realizar ese respaldo, además donde se almacenan los respaldos es en el mismo lugar, haciendo vulnerable su perdida ante algún daño físico de disco duro.

Existen muchas formas e implementaciones con los lenguajes de base de datos SQL disponibles además en sistemas Linux y Windows. MySQL y MariaDB son dos opciones económicas y populares que se las usa para implementar bases de datos relacionales en entornos de servidor, que son con las que cuenta ISANET, sin embargo, estas herramientas suelen ser pasivas en lo que corresponde a la seguridad, si es que estas no están configuradas de forma adecuada.

Para simplicidad, se puede mencionar que, como recomendación luego del análisis de los expertos y de la autora, se anexa (ANEXO 2) una serie de scripts o pasos en el servidor, para que este ambiente sea netamente seguro

La seguridad de los operadores de Internet isp

Como todos saben en este tiempo(año), ha habido muchos cambios. Actualmente muchas personas hacen uso del internet generalmente se conectan utilizando enrutadores domésticos para teletrabajo, estudio o navegación. Es ahí donde debe intervenir la seguridad de los operadores ISP y obtiene una mayor notabilidad o relevancia en las personas. El punto es si la seguridad del ISP sería tan eficaz como para llegar a hacer la única que necesiten las empresas y sus teletrabajadores. (Carolina Bonilla;, 16)

Se conectan más a internet desde los hogares

Debido a esta pandemia más conocida como el Covid-19 ha causado un cambio muy radical en nuestras vidas tanto como en el ámbito laboral y de sobrevivencia. Es decir, ha cambiado nuestra forma de trabajar y también de vivir. Actualmente muchas de las personas que cuentan con un empleo trabajan de forma remota desde sus viviendas, debido al covid-19 o porque antes ya trabajan de esa forma. Estas personas son totalmente dependientes de su operador de internet, solo así podrán realizar su trabajo diario. (ambit team;, 2020)

¿La seguridad de los operadores de Internet es suficiente para la empresa y el hogar?

Un dato importante es saber que los operadores de internet o ISP no son reconocidos por la protección de seguridad. Aunque, hay información de que la mayoría de ellos aseguran que están ampliando sus defensas frente a los ataques de los cibercriminales suelen cometer, como, por ejemplo, teniendo una división específica de ciberseguridad o también contratando un hardware o un soporte técnico de empresas que fuertemente se dedican a estos menesteres de la seguridad informática. (Manuel Gómez Martinez;, 17)

Según Vince Crisler, Alto directivo de Dark Cubed y ex director de seguridad informática en la Casa Blanca - USA, argumenta que, es que la seguridad para pequeñas y medianas empresas y los usuarios en hogares un principal factor por lo cual intervenir.

Razones por las que una protección de seguridad de un ISP no es suficiente

Crisler comento que este problema es recurrente en muchos lugares, y se debe a que las empresas ISP se concentra de forma primaria en ofrecer un servicio de internet con su ancho de banda confiable y seguro para sus clientes, sin distinguir el uso que le den o el tráfico que circule en sus redes. De igual manera comenta que los ISP priorizan estas 2 cuestiones por encima de todo el resto. En sí, si requirieran tomar una decisión entre la debida seguridad y tiempo de actividad sin duda su decisión sería en que se enfocarían en el tiempo de actividad. (DOMINIOS DE LAS CIENCIAS;, 2019)

Otro tema que se debe tener presente es que debido a que los ISP siempre brindan un hardware doméstico con frecuencia es obsoleto y no cuenta con una protección, ya que este cuenta con diferentes debilidades en dos casos como lo son la seguridad y los softwares antiguos. Cabe recalcar que varios de los clientes utilizan hardware de red de su ISP. De esta manera, estos dispositivos como los routers, con frecuencia carecen de controles de seguridad básicos. Una de la problemática se encuentra en que no reciben las correctas actualizaciones los equipos por parte de firmware e inclusive se dice que firmware suele dejar desprotegido los servicios telnet y las diferentes administraciones de web. (DOMINIOS DE LAS CIENCIAS;, 2019)

Sin embargo, los ISP se protegen expresando que los debidos problemas de seguridad no dependen únicamente de ellos. Pero también es cierto, que debido a las

expectativas altas que tienen los clientes, eso no les quita que deban de mejorar. (DOMINIOS DE LAS CIENCIAS;, 2019)

Que se puede hacer para mejorar la seguridad del ISP

Shrihari Pandit, él es el presidente y director ejecutivo de Stealth Communications, cuenta con un pensar que la mejor manera de solucionar esto, es que deberían hacer cambios en las capas de comunicación OSI. (redeszone, 2020)

En la **Capa 1 / Capa física**, unos de los problemas más cotidiano del ISP es que no existen cifrado entre el ISP y el usuario/cliente. Esto de torna peligroso para es los respectivos proveedores que ofrecen el servicio a través de las tecnologías inalámbricas o de fibra PON. A todos los suscriptores estas tecnologías transmiten trafico además permiten a los atacantes acceder físicamente a la red. En España los ISP de FTTH utilizan grandemente el estándar GPON, y también hacen el utiliza las Advanced Encryption Standard más conocidas como AES. (redeszone, 2020)

En la diferencia que la **capa 2 / también conocida como la Capa de enlace de datos (Ethernet)**, esta es encargada de representar la comunicación entre los implicados en este caso la ISP y el usuario/cliente, como anteriormente ya fue mencionado este servicio no encripta el tráfico, además de ser muy abierto a la investigación/espionaje. Una de las maneras de poder manejar mejor la seguridad en los sitios correspondientes seria efectuando tecnologías más avanzadas como las de MACsec ya que son muy reconocidas y muy buenas en su función. (redeszone, 2020)

En la capa 3 / Capa de transporte (Protocolo de Internet) tanto como los usuarios y también las organizaciones pueden implementar IPsec para hacer las cosas más fáciles para la requerida encriptación entre los diferentes extremos. De esta manera se lograra

efectuar que los delincuentes/ciberdelincuentes tengan problemas al querer tener acceso, de esta forma no podrán decodificar el tráfico que se realiza entre los proveedores y su internet. Deben implementar el uso de los VPN, y así poder agregar una adicional capa de seguridad. (redeszone, 2020)

Equipos de seguridad para ISP

Seguridad de Sistema de Detección de Intrusos - IDS aquí las políticas se separan en dos puntos que son Implementación y Administración, esto nos ayudará a que sean definidas correctamente las funciones del personal. Estas políticas IDS deben contener como mínimo los siguientes puntos: (Manuel Gómez Martinez, 2017)

Implementación

Los debidos procesos de logging de las aplicaciones y sus sistemas operativos deben estar activados en todos los hosts y servidores.

La alerta de los firewalls, alarmas y otros dispositivos de control de acceso al perímetro deben estar activados. (Manuel Gómez Martinez, 2017)

Los Procesos de auditorías periódicas para la revisión de los procesos, control y revisión de los IDS.

Administración

Para la revisión dela integridad de los sistemas de ficheros de firewalls se debe instalar el IDS y también para otros sistemas de control de acceso al perímetro.

También es recomendable revisar diariamente los logs en los sistemas de control de acceso al perímetro y periódicamente los logs de los hosts y asimismo a los servidores que están situado en la red interna.

Serán muy bien revisados todos los problemas que reciban los administradores, en busca de alguna actividad intrusa. Estas estrategias son las más mínimas que debe de tener en cuenta una empresa como para una seguridad básica. Estos procedimientos suelen ser usados normalmente en organizaciones o empresas que tienen Riesgos Bajos. (Manuel Gómez Martinez, 2017)

¿Qué es un Firewall?

Un firewall en Mikrotik puede ser hardware, software o ambos, este es el encargado de establecer una barrera entre una red interna (LAN) y una red externa, por ejemplo el internet. El firewall se encarga de monitorear tanto como el tráfico de red entrante y el tráfico de la red saliente, este también se encarga de decidir si permite o bloquea el tráfico específico en función de una cadena de reglas de seguridad esto es lo que nos ayuda a mantener integra la información que pasa por nuestra red. (geekland, 2013)

En el Mikrotik logramos hallar 3 tipos de cadenas las cuales permiten declarar en que momento será aplicada una regla respecto a si será el trafico entrante, saliente o también todo el tráfico que suele pasar por nuestra red.

Input: Es decir, todo lo que entra al router, desde cualquier interface, además de ser un tráfico de entrada un ejemplo claro podría ser cuando le das ping a la interface desde un pc.

- Output: Es todo lo que sale desde el router a través de una interface, por ejemplo, es cuando das ping desde tu terminal del router hacia afuera, pueden ser los DNS de google 8.8.8.8, un dominio en especial o también hacia la computadora.

- Forward: aquí es todo lo que atraviesa al router, en cambio en este se puede tener 2 o más interfaces. Por ejemplo, es cuando das ping desde una red a otra red, es un tráfico que ingresa y sale.

Las bases de datos y su seguridad

El mayor porcentaje de los diferentes datos sensibles (del mundo entero) se encuentra guardados y almacenados en los gestores de las bases de datos una de las mas reconocidas es Oracle, también otra de ellas es Microsoft SQL server en otras más.

Para atacar una de estas bases de datos o ya sea otras se a ha vuelto un objetivo para los delincuentes de datos. Pero la explicación que se ha llegado a conocer de porque suelen atacar mucho a este punto en específico es porque cuentan con victoria es decir éxito en las diferentes páginas web que se encuentran vulnerables, esto se ha vuelto en un beneficio para ellos.

Para agregar un estudio del año 2009 publicado por The Independent Oracle Users Group reconocido por sus siglas IOUG nos comenta que la media parte de los usuarios de la compañía de Oracle constan con dos parches pero sin emplear en sus distintos manejadores.

Un punto importante la cual se concentro es en mantener seguro los perímetros de las redes los que fueron más posibles, esto se logro por medio de firewalls, los antivirus y también los IDS/IPS. Esto se da para proteger las bases de datos, solo de esta manera se concibe proteger la seguridad de los intrusos no deseados o como también de cambios que no han sido autorizados.

En las otras partes encontraremos lo que son las recomendaciones para proteger una base de datos en instalaciones tradicionales. (Manuel Gómez Martinez, 2017)

Identifique su sensibilidad

Para comenzar deben de confeccionar deben de crear una tabla donde den a conocer cuáles son los datos más vulnerables o sensibles de sus diferentes bases de datos. Igualmente, ay que tomar en cuenta que automatizar los distintos procesos como por ejemplo el proceso de identificación, es muy importante por motivo de que tanto los datos como las ubicaciones casi siempre se encuentran en cambios por motivo de las nuevas aplicaciones o también los cambios de producto de fusiones y adquisiciones.

Además, deben de desarrollar o obtener herramientas de identificación, para asegurar éstas contra el malware, otro punto es que deben de colocar el resultado de ataques en la base de datos; porque muy aparte de dejar expuesta las otras informaciones, de igual forma esto deja abierta la posibilidad a los delincuentes de incorporar nuevas estrategias de robo a las bases de datos.

Evaluación de vulnerabilidad y configuración

Evaluar las bases de datos y su respectiva configuración, sirve para asegurarse que no tiene vacíos de seguridad.

Para empezar, se hace una instalación de la correspondiente base de datos y su debido sistema operativo luego de este proceso se requiere una verificación, un ejemplo de lo que se debe verificar es la comprobación de la base de datos y su ejecución. (welivesecurity, 2014)

De la misma forma, con archivos con parámetros de configuración y programas ejecutables.

Es muy importante, que hagan la debida verificación para que se den cuentan que no se está realizando la ejecución de versiones las cuales estás constan con debilidades para nuestra base de datos. En siguientes puntos mostramos como impedir consultas de SQL:

- Primer punto, se debe poner límites al acceso esto va dirigido al cliente.
- Segundo punto, también limitar el acceso tanto como a los datos/clientes/procedimientos.
- Tercer punto, Disminuir el encuentro de horas entre los clientes.

Endurecimiento

Después de haber hecho la evaluación correctamente de vulnerabilidad se ofrece ciertas comisiones. Este es el punto número uno en el que se da el endurecimiento de la base de datos. Otro elemento de endurecimiento que hace referencia es la eliminación aquí se trata de eliminar cosas que no tengan tanta importancia o utilización como lo son ciertas funciones y opciones. Además de esto se crea reglas donde se explica que se debe hacer y que no. (geekland, 2013)

Audite

Después que hay hecho la respectiva creación de configuración y controles de endurecimiento, habría de realizar auto evaluaciones y un pertinente seguimiento a las recomendaciones de auditoría para que de esta manera se esté asegurando que no se está creando caminos incorrectos e innecesarios, que en este caso es la seguridad que tiene la prioridad.

Hay que agilizar un registro en la configuración donde los diferentes tipos de cambios que se realice quede automáticamente quede registrado. Algo necesario es Implementar alertas sobre cambios en la configuración. Un punto muy a tomar en cuenta es que cuando se realiza un cambio o varios cambios estos consiguen afectar a lo que la seguridad (base de datos). (geekland, 2013)

Monitoreo

Monitorear en tiempo actual las diferentes actividades de una base de datos es un punto clave para definir su exposición, se requiere aplicar o adquirir agentes inteligentes de monitoreo, además detección de intrusiones y uso indebido.

Un ejemplo, son cuando existen alertas por ejemplo de los patrones inusuales de acceso, cuando hay presencia de este tipo de alerta puede ser un ataque de inyección SQL, estos generan cambios que no cuentan con autorización tanto como en los datos o también podría ser en las cuentas.

Ten en cuenta que hacer el debido monitoreo de todos los clientes/usuarios con privilegios se ha convertido en una obligación por parte de la gobernabilidad de datos algo más son los cumplimientos de regulaciones como SOX y regulaciones de privacidad. Además, esto nos ayuda a poder detectar delitos.

Se debe tomar en cuenta que el monitoreo dinámico es también un componente principal de la evaluación de vulnerabilidad, ya que este conoce más de las evaluaciones

entre otros más temas. Por ejemplo, lo encontramos cuando ocurre privilegio o cuando hay exceso de inicio de sesión en la BD. (geekland, 2013)

Autenticación, control de acceso, y Gestión de derechos

La creación tanto como de los clientes y sus datos no contienen la misma información. Es decir, ninguno es igual, todos cuentan con algo personal. La responsabilidad de cliente/usuario es tener algo propio en sus claves. Pero la empresa debe de garantizar la rendición de cuentas por consumidor/usuario, y también poner límites de acceso de los datos a usuarios que requieren ciertas excepciones.

Una recomendación es tener un periodo la cual se haga revisiones sobre los informes de derechos de los clientes/usuarios, esto sería un punto correcto por parte de la auditoria.

También, deben manejar el cifrado para lograr hacer ilegibles los datos confidenciales, de esta manera los delincuentes lo tendrán más difícil, solo así se logrará proteger el cifrado de datos, la capa de red y también no logra tener camino a los envíos por parte del usuario hacia la data base. (escuelaeuropeaexcelencia, 2019)

La estrategia de seguridad en relación con las bases de datos

Uno de los principales objetivos de los ataques informáticos han sido siempre las bases de datos, se trata de un botín muy interesante y preciado para los delincuentes de la red, ya una mina de oro en la era de internet, significa mucho poder. En los actuales días, lo que se necesita es equipar a las organizaciones de estrategias coherentes y agiles para reducir vulnerabilidades y actuar fuerte contra los posibles ataques, pero

además se debe mantener un régimen reglamentario en cuestiones de seguridad y privacidad. De esta manera, deben tomarse todas las medidas correspondientes para mantener a buen recudo la información de las organizaciones. (biblioguias, 2020)

El grado de importancia de la seguridad en relación con las bases de datos

La información de las organizaciones grandes o pequeñas, siempre mantienen bases de datos, para cualquier tipo de sistemas de información, por lo que se soporta en sistemas administradores de gestión de datos tales como Microsoft SQL, MySQL, MariaDB, Oracle, entre otros. Es esta información la que suele motivar a los atacantes pretender acceder a esos servidores de bases de datos y de esta manera poder tomar información que puede ser financiera, técnica, de clientes y que, al perderla, una empresa puede sufrir graves consecuencias.

Los Atacantes suelen hacer uso de diferentes técnicas para aprovecharse de vulnerabilidades que pueda tener un sistema de bases de datos, por lo que podría ser por algo tan sencillo como poseer una política débil de contraseñas, también la falta de actualización de software o la manera de configuración de acceso que tengan a los sitios empresariales. (digitalguideionos, 2019)

Lo importante siempre será mejorar la seguridad perimetral de todos los servicios informáticos con equipamiento de punta, que cuenten con buen procesamiento y algoritmos adecuados en forma de dispositivos así con firewalls, IDS/IPS y antivirus; si se quisiera comparar a la vida real, sería el de llegar a tratar a nuestro servidor como una fortaleza, rodeada de paredes con muros impenetrables y defensas avanzadas. Sin embargo, ha quedado demostrado que aun con eso no es suficiente, pues deben generarse nuevos mecanismos de defensa, que implican además construir ambientes con

políticas y estrategias de seguridad que además generen compromisos con los empleados. (digitalguideionos, 2019)

Las vulnerabilidades que más frecuentemente se encuentran en las bases de datos

Contraseñas débiles

No es difícil encontrarse con administradores de bases de datos que en la actualidad siguen utilizando contraseñas de acceso a servidorres y consolas de bases de datos muy comunes como escribir: admin/12345; lo único que causa esto es que convierte el acceso a los servidores en el eslabón más débil dejando su protección abierta contra los ataques. Debido a este problema deben centrarse en una creación de contraseñas complicada y segura que lleve tantas letras, números, caracteres como sea necesario. (biblioguias, 2020)

Preferencia de privilegios de usuario por privilegios de grupo

En muchas de las situaciones, hay usuarios que cuentan con más privilegios de los que solicitarían, esto es un gran con conveniente y un seguro agujero en la seguridad. Por eso deben de cambiar esta situación de los y definir los roles y accesos debidamente necesarios. Un escenario de esto podría ser, que un único usuario se limite a las consultas, y no a realizar inserciones ni actualizaciones. (Manuel Gómez Martinez, 2015)

Cabe indicar que, con cada instalación de una base de datos, suelen instalarse software adicionales y librerías que no suelen ser utilizadas. Entonces estos paquetes quedan sin ser actualizados, también son olvidados y estos pueden resultar ser puertas de acceso a un ataque. Para disminuir los riesgos, se recomienda que los usuarios deben

de detectar esos paquetes olvidados y procedan a su desactivación para reducir ese riesgo. (Manuel Gómez Martinez, 2015)

Bases de datos desactualizadas y sin cifrar

Es algo valioso contar con bases de datos seguras, con cifrado adecuado, para no tener problemas con los secuestros y robos de información, hay que especificar que cuando se realizan actualizaciones pueden bajarse además software malicioso relacionado con afectar las vulnerabilidades, pero también pueden ofrecer defensas a esos posibles puntos débiles.

También, no todas las entidades o compañías suelen cifrar la información almacenada en una base de datos. Como todos saben el cifrado es una de las maneras de evitar que, en caso de hackeo y robo, esa información pueda ser compartida. (Manuel Gómez Martinez, 2015)

SQL Inyection

Siendo este es uno de los ataques que con más frecuencia se ha reportado, y es el resultado de las vulnerabilidades de las bases de datos por culpa de los sistemas mal desarrollados. Además, un mal desarrollo de software, puede hacer ejecutar código malicioso y tomar el control de todo un sistema o la base de datos completa. (digitalguideionos, 2019)

Recomendaciones para la protección de una base de datos

Identificar todas sus vulnerabilidades reportadas

Se deben evaluar y analizar las configuraciones de una base de datos y además de reconocer las debilidades del sistema operativo donde esta funciona.

Realizar una auditoría

Ya que se ha creado una configuración totalmente segura, deben realizar la reconocida auditoría para estar más seguros de que ha seguido la hoja de ruta marcada para así garantizar la seguridad de la base de datos.

Ten el software siempre actualizado

El tener a el sistema en último momento es una de las vulnerabilidades más fáciles de corregir. Debido a esto, deben instalar los conocidos parches de seguridad del sistema, los parches deben ser lo que te permitan tapar agujeros de seguridad y al mismo tiempo que te permita garantizar que nunca sufras de ataques.

Vigilancia absoluta de todas las acciones y procesos en relación a las bases de datos

Es muy importante conocer que un monitoreo de la base de datos les ayudara a saber si en algún caso, la base este siendo usada sin autorización o alguna persona con autorización está realizando alguna operación no programada.

Supervisar los accesos

Debemos aclarar que no todos los datos son iguales, ni tampoco que todos los usuarios deben acceder a las mismas operaciones en un sistema, existen escalas y roles jerárquicos de acceso que deben configurarse. Sin embargo, siempre se ha reportado

violaciones a las seguridades en relación a estas malas prácticas, ya que cuentan con acceso y privilegio completo usuarios que realmente no los necesitan.

CONCLUSIONES

Los proveedores de internet deben ser los primeros que demuestren una seguridad robusta no es posible que la empresa que provee a internet se ha vulnerada, ya que esto podría representar desproteger de esta manera a sus clientes o sería claramente un indicador de que no está posibilitada para su protección.

Lo importante es mejorar la seguridad de cualquier tipo de servicio informático como una base de datos, a través del aseguramiento perimetral, esto es con equipos destinados para estas funciones, tales como: firewalls, IDS/IPS y antivirus.

Es necesario que los ISP creen nuevos tipos de defensas como son las estrategias de protección del equipo final y la utilización de políticas que ayuden a mejorar esos esfuerzos de seguridad.

Es muy común observar que, para brindar seguridad dentro de los ISP, es que se utiliza hardware doméstico, que les representa una falsa protección, porque al tener equipos o infraestructuras de bases de datos o redes detrás de dispositivos de configuración básicas, que son fabricados para el hogar, estos se tornan vulnerables ante intrusiones y ataques.

Es vital e importante además que los ISP protejan sus bases de datos y sobre todos los sistemas con los que se conectan los usuarios, estos son vulnerables a los ataques de injection SQL.

Bibliografía

ambit team;. (20 de 11 de 2020). *ambit-bst.com*. Obtenido de ambit-bst.com: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

biblioguias. (18 de 12 de 2020). *biblioguias.cepal.org*. Obtenido de biblioguias.cepal.org: https://biblioguias.cepal.org/c.php?g=495473&p=4398100

Carolina Bonilla;. (29 de 12 de 16). *Tesis_t1200mbd.pdf*. Obtenido de Tesis_t1200mbd.pdf: https://repositorio.uta.edu.ec/bitstream/123456789/24534/1/Tesis_t1200mbd.pdf

digitalguideionos. (2019). *ionos.es*. Obtenido de ionos.es: https://www.ionos.es/digitalguide/servidores/seguridad/bases-de-datos-la-importancia-de-asegurar-tu-informacion/

DOMINIOS DE LAS CIENCIAS;. (2 de 09 de 2019). *archivolocalocompartido*. Obtenido de archivolocalocompartido: file:///C:/Users/peher/Downloads/Dialnet-AnalisisDeRiesgoYVulnerabilidadesDeLaRedDeDatosEnU-7164360.pdf

escuelaeuropeaexcelencia. (09 de 2019). *escuelaeuropeaexcelencia.com*. Obtenido de escuelaeuropeaexcelencia.com: https://www.escuelaeuropeaexcelencia.com/2019/09/como-gestionar-los-controles-de-acceso-segun-iso-27001/

geekland. (6 de 07 de 2013). *geekland.eu*. Obtenido de https://geekland.eu/que-es-y-para-que-sirve-un-firewall/

Manuel Gómez Martinez. (12 de 03 de 2015). *vulnerabilidades-bbdd-wp-acens.pdf*. Obtenido de vulnerabilidades-bbdd-wp-acens.pdf: https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

Manuel Gómez Martinez. (2017). WHITEPAPER. En M. G. Martinez, *vulnerabilidades-bbdd-wp-acens* (pág. 5). acensTechnologies. Obtenido de Martinez, Manuel Gómez.

Manuel Gómez Martinez;. (15 de 03 de 17). *acens.com*. Obtenido de acens.com: https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

redeszone. (9 de 2020). *redeszone.net*. Obtenido de redeszone.net: https://www.redeszone.net/noticias/ofertas/routers-dispositivos-wifi-amazon-septiembre-21/

villalobos, johonny;Vulnerabilidad de Sistemas Gestores de Bases de. (2017). *repositorio.uta.edu.ec*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/24534/1/Tesis_t1200mbd.pdf

welivesecurity. (12 de 11 de 2014). *welivesecurity.com*. Obtenido de welivesecurity.com: https://www.welivesecurity.com/la-es/2014/11/12/identificar-analizar-evaluar-vulnerabilidades/

ANEXO 1

ENTREVISTA A EXPERTOS, FORMULARIO DE PREGUNTAS

EN RELACION A: ANÁLISIS DE VULNERABILIDAD DE LA BASE DE DATOS EN LA EMPRESA ISANET DEL CANTON MONTALVO

NOMBRE: ING JOFFRE NAVARRO

FECHA:8/09/2021

¿Qué entiende por análisis de vulnerabilidad aplicada a una empresa proveedora de servicio de internet?

Se trabaja con servicios Linux con los servidores de los usuarios

¿Basada en su experiencia relata cómo es posible determinar una base de datos sea segura?

La seguridad de mantener respaldo de las bases de datos de acuerdo a las necesidades en caso de la falle técnica o falla de hardware

¿Cómo cree usted que se pueda evitar la vulnerabilidad de una base de datos?

Poner una seguridad al inicio de un dispositivo o servidor

¿Qué herramientas podemos utilizar para el análisis de vulnerabilidad de una base de datos?

Basados en sistemas no tan comunes como Linux ventanas que no mantengan ventanas de diseño incluyendo su propia seguridad tanto en la programación como dispositivo

¿Qué importancia tiene la prevención del análisis de la base de datos?

Sumamente importante si una base de datos se llega a distribuir pierde el 100% de su trabajo y volverá a realizar, abría asuntos internos que no se podría corregir al tiempo de trabajo

ENTREVISTA A EXPERTOS, FORMULARIO DE PREGUNTAS

EN RELACION A: ANÁLISIS DE VULNERABILIDAD DE LA BASE DE DATOS EN LA EMPRESA ISANET DEL CANTON MONTALVO

NOMBRE: ING DALILA VARGAS

FECHA:10/09/2021

¿Qué entiende por análisis de vulnerabilidad aplicada a una empresa proveedora de servicio de internet?

Existen ataques o debilidades como reaccionamos a priorizar vulnerabilidades y priorizar las vulnerabilidades ante cualquier ataque o clon de bases de datos

¿Basada en su experiencia relata cómo es posible determinar una base de datos sea segura?

Que no tenga fugas de información

¿Cómo cree usted que se pueda evitar la vulnerabilidad de una base de datos?

Evitando la fuga de información, generalmente es cuando venden la información de la base de datos.

¿Qué herramientas podemos utilizar para el análisis de vulnerabilidad de una base de datos?

Diseño de seguridad subiendo a la nube en lugar que no sea vulnerable siendo siempre confiable y teniendo una contraseña segura

¿Qué importancia tiene la prevención del análisis de la base de datos?

Depurar, verificar evitar clonaciones crear en fox y aplicaciones seguras

ANEXO 2

Recomendaciones para ejercer seguridad técnica en la base de datos MYSQL:

Vamos a ingresar los comandos en esta sección en la interfaz de solicitud de MySQL, por lo que debemos iniciar sesión.

```
mysql -u root -p
```

PROTECCIÓN DE CONTRASEÑAS Y ASOCIACIONES ANFITRIONAS

Primero, asegúrese de que no haya usuarios sin una contraseña o una asociación de host en MySQL:

```
SELECT User,Host,Password FROM mysql.user;
```

Podemos establecer una contraseña para el usuario con este comando. Cambia " newPassWord " para reflejar la contraseña que deseas asignar.

```
UPDATE mysql.user SET Password=PASSWORD('newPassWord') WHERE
User="demo-user";
```

Si miras en el campo "Host", verás que todavía tenemos un "%", que es un comodín que significa cualquier host. Esto no es lo que queremos. Cambiemos eso para ser "localhost":

```
UPDATE mysql.user SET Host='localhost' WHERE User="demo-
user";
```

Si comprobamos nuevamente, podemos ver que la tabla de Usuario ahora tiene los campos apropiados establecidos.

```
SELECT User,Host,Password FROM mysql.user;
```

Si nuestra tabla contiene algún usuario en blanco (no debería en este punto ya que ejecutamos "mysql_secure_installation", pero cubriremos esto de todos modos), deberíamos eliminarlos.

Para hacer esto, podemos usar la siguiente llamada para eliminar a los usuarios en blanco de la tabla de acceso:

```
DELETE FROM mysql.user WHERE User="";
```

Una vez que hayamos terminado de modificar la tabla de Usuario, necesitamos ingresar el siguiente comando para implementar los nuevos permisos:

```
FLUSH PRIVILEGES;
```

IMPLEMENTACIÓN DE USUARIOS ESPECÍFICOS DE LA APLICACIÓN

Similar a la práctica de ejecutar procesos dentro de Linux como un usuario aislado, MySQL se beneficia del mismo tipo de aislamiento.

Cada aplicación que usa MySQL debe tener su propio usuario que solo tiene privilegios limitados y solo tiene acceso a las bases de datos que necesita para ejecutarse.

Cuando configuramos una nueva aplicación para usar MySQL, deberíamos crear las bases de datos que necesita esa aplicación:

```
create database testDB;

Query OK, 1 row affected (0.00 sec)
```

Luego, deberíamos crear un usuario para administrar esa base de datos y asignarle solo los privilegios que necesita. Esto variará según la aplicación, y algunos usos necesitan más privilegios abiertos que otros.

Para crear un nuevo usuario, use el siguiente comando:

```
CREATE USER 'demo-user'@'localhost' IDENTIFIED BY 'password';
```

Podemos otorgar los nuevos privilegios de usuario en la nueva tabla con el siguiente comando. Consulte el tutorial sobre cómo crear un nuevo usuario y otorgar permisos en MySQL para obtener más información sobre privilegios específicos:

```
GRANT SELECT,UPDATE,DELETE ON testDB.* TO 'demo-
user'@'localhost';
```

Como ejemplo, si luego necesitamos revocar los privilegios de actualización de la cuenta, podríamos usar el siguiente comando:

```
REVOKE UPDATE ON testDB.* FROM 'demo-user'@'localhost';
```

Si necesitamos todos los privilegios en una determinada base de datos, podemos especificar eso con lo siguiente:

```
GRANT ALL ON testDB.* TO 'demo-user'@'localhost';
```

Para mostrar los privilegios actuales de un usuario, primero debemos implementar los privilegios que especificamos usando el comando "privilegios de descarga". Luego, podemos consultar qué otorga un usuario:

```
FLUSH PRIVILEGES;

show grants for 'demo-user'@'localhost';
```

CAMBIO DEL USUARIO ROOT

```
rename user 'root'@'localhost' to 'newAdminUser'@'localhost';
```

Podemos ver el cambio utilizando la misma consulta que hemos estado usando para la base de datos del usuario:

```
select user,host,password from mysql.user;
```

Nuevamente, debemos eliminar los privilegios para que estos cambios ocurran:

```
FLUSH PRIVILEGES;
```

Recuerde que deberá iniciar sesión en MySQL como el nombre de usuario recién creado de ahora en adelante cuando desee realizar tareas administrativas:

```
mysql -u newAdminUser -p
```

CONCLUSIÓN DE LOS EXPERTOS

La vulnerabilidad de la empresa no se vende ni se filtra la información de los clientes porque es una información personal ya que la empresa segura siempre el acceso a la base de datos es un personal destacado de la misma empresa.

La empresa cuenta con una sola base de datos donde abarca a todos sus clientes con sus respectivas informaciones ya que cuenta con un respaldo cien por ciento seguro y con una barrera adicional al ingresar solo ingresan los creadores de dicha base de datos