Actividad [#2] – [Vulnerabilidades de comunicación] [Seguridad informática 1]

Ingeniería en Desarrollo de Software

Tutor: Elizabeth Guevara Roa

Alumno: Manuel Enrique Ramirez Lopez

Fecha: 19/04/2022

Indice

Bases de datos

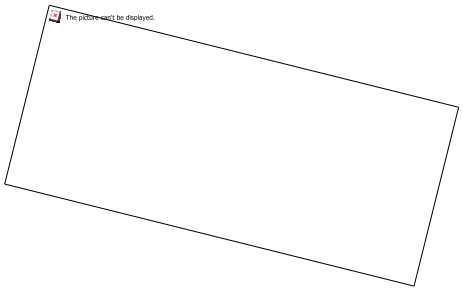
Recomendaciones

-Solo personal autorizado puede acceder a los servidores físicos, a su vez aislar completamente en una sala o piso los servidores y reforzar los accesos, que en las entradas y salidas se tome captura de huellas, iris y tarjeta electronica de identificación del personal que acceso a dicha sala.

-Al momento de diseñar las instalaciones tomar en cuenta factores externos que puedan llegar a afectar dicha instalación como pueden ser riesgos naturales como en este caso lo son los tsunamis y o terremotos, colocarlo de manera estragica para salvaguardar toda la informacion.

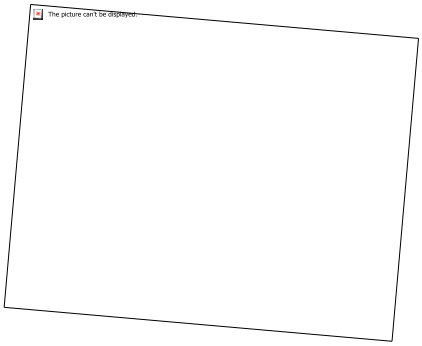
-Contar con respaldos en caso de perdida total del centro principal, con esto implementar las mismas medidas que se mencionaron en los puntos anteriores pero esta vez en una locación mas segura centricamente donde los factores externos (sociales y naturales) sean mínimos.

-Nombres de usuarios y contraseñas seguros y no fáciles de adivinar, es decir no poner datos que sean fáciles de identificar como podrían ser que tu contraseña sea la fecha de tu cumpleaños, tomar en cuenta apartados de datos irreconocibles o al menos que les tome bastante tiempo lograr descifrarlos.



DNS

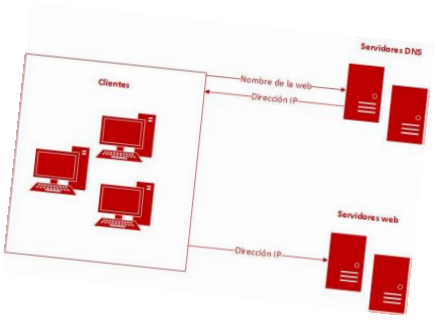
Recomendaciones



-Crear un nombre de dominio fácil de ubicar, es decir es mas fácil recordar “miclinica.com” a “ClinicaGutierrez99.net” con esto logramos que nuestra dirección IP sea mas sencilla de ubicar y así evitamos una suplantación de dominio.

-Contar o hacer que tus clientes sigan tus distintas paginas ya sea Facebook, twiter linkedin o hasta mas personal via chat en whatsapp, ¿Con que fin? Si llegamos a sufrir algun ataque DoS (Denegación de servicio) donde inutilice nuestro sitio web principal y causar confucion con nuestros clientes tener la oportunidad de mantenerlos informados cuando se haya parado el ataque y puedan volver a ingresar a nuestros servidores todo esto de forma “Online” y si hablamos de forma local es decir que algun colaborador no pueda acceder a ningún servicio por lo mismo del ataque y gracias a la copia de seguridad periódica podemos acceder a un modo local con los registros de la copia de seguridad y con la oportunidad de seguir brindando servio aunque en menor medida.

-Dentro de las instalaciones asignar una dirección única que coincida con el metodo de acceso a la red principal , es decir como esta constituida la instalación 21 estaciones de trabajo a la cual a cada una de ellas se les dará un acceso eh identificador para darle “x” derechos de acceso mientras que los de la segunda planta se conectan via Wifi y no están identificados cuantos equipos se quieren conectar, debemos saber el numero exacto de conexiones y equipos para garantizar que no haya equipos infiltrados que puedan acceder a toda la instalación y su informacion.



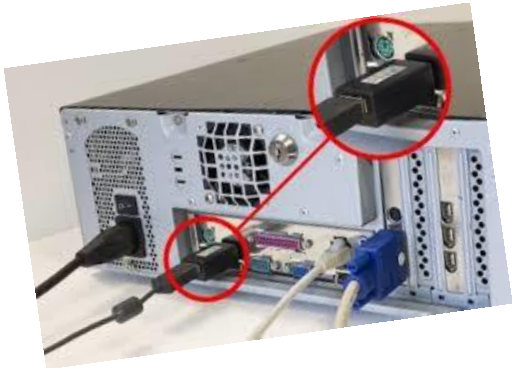
KeyLogger

Recomendaciones

-Poner como regla o bloquear puertos USB de cada estacion de trabajo y dejar unicamente las indispensables para su uso con esto evitamos que se infecte por medio físico que viene siendo la manera mas fácil y tentadora de hacerlo.

-Restringir acceso a internet a cada estacion de trabajo, es decir no permitir el uso “común” de dispositivos que son de uso exclusivo del trabajo y así evitamos que por medio de paginas externas o de dudosa procedencia se descargue algun malware o caballo de troya que comprometa la seguridad y integridad de la informacion.

-Siempre usar software oficial, es decir que no este alterado para desbloquear funciones de paga, es mejor contemplarlo en el gasto de la empresa ese pequeño extra de uso de software oficial a usar algun tipo de herramienta que lo desbloquee “gratis” y que este mismo pueda afectar o desplegar malware.

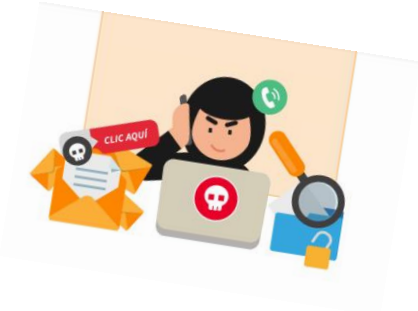


Ingeniería social

Recomendaciones

-Colocar letreros de advertencia sobre no insertar o colocar dispositivos externos a las estaciones de trabajo, con esto evitamos caer en algun “anzuelo” de algun hacker que quiera hacer daño a la informacion almacenada y a los equipos.

-Platicas de seguridad o prevención de ataques, que van desde las tecnicas mas usadas por los atacantes que son las de Phishing, pretextos y así nos sercioramos que cada uno de nuestros colaboradores están calificados para evitar caer en fraudes.



-Quid pro quo, que se refiere a algun cambio justo, es decir que algun atacante se haga pasar por alguien de “confianza” o técnico externo que viene a hacer mantenimiento prometiendo mejorar el sistema, y así aprovecharse de la vulnerabilidad humana de confiar en alguien.

Bibliografía

Enrique Lopez. (2021). Seguridad Ataques DNS: qué son y cómo protegernos. 2022, de Privada Sitio web: https://www.redeszone.net/tutoriales/seguridad/consejos-evitar-ataques-dns/

Enrique Lopez. (2021). Qué es un Keylogger y cómo protegerse de un Keylogger. 2022, de Privada Sitio web: https://blog.mailfence.com/es/protegerse-de-un-keylogger/

Enrique Lopez. (2020). Maneras de evitar ataques de ingeniería social. 2022, de Privada Sitio web: https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks