TRABAJO PRACTICO N° 3

Alumno: Diaz Exequiel

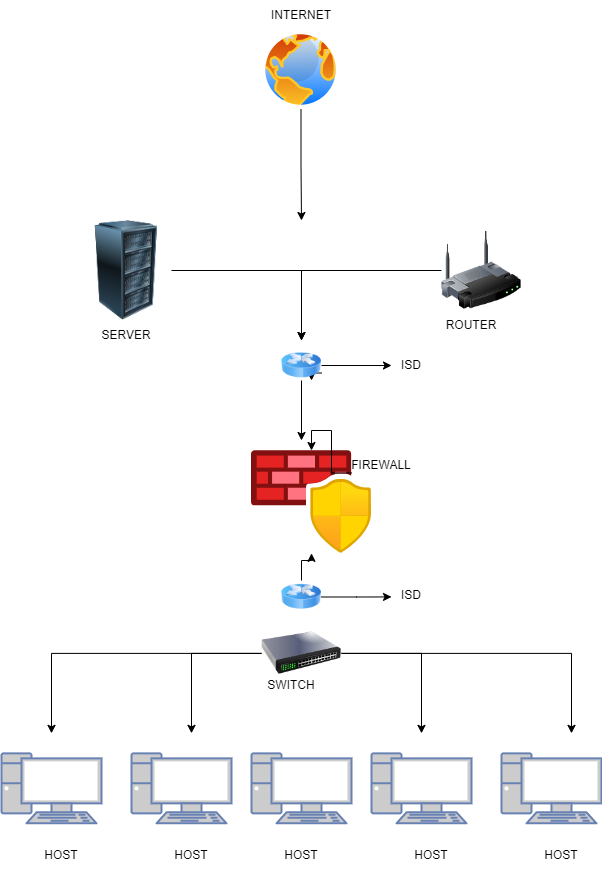
Tutor : Carlos Mendez

Informe de Perímetro - Ransomware ShinoLocker

El Ransomware ShinoLocker tiene como objetivo la encriptación de información debido a esto es que se hace casi imposible recuperar esa información encriptada sin tener que abonar una suma de dinero o algún otro bien. Realizar el pago no siempre es un indicativo de que la persona que realizo la acción de la encriptación de la información nos vaya a dar la clave de desbloqueo. A raíz de este ataque sufrió al empresa Luxor en día 28 de Septiembre del 2022 es que se recomienda llevar a cabo las siguientes acciones.

* Fortalecer las medidas de seguridad de la red teniendo siempre actualizados los sistemas con los últimos parches de seguridad.
* implementar sistemas de detección de intrusos (IDS) con el fin de monitorear el trafico de datos que se transfieren entre redes publicas y privadas.
* Introducir también sistemas de prevención de intrusiones (IPS)con el fin de filtrar los paquetes de datos que se van a recibir o no.
* Colocar FIREWALL que sean capas de filtrar la información a las que los empleados de la empresa puedan acceder. Dar un manejo libre de internet a los empleados es un error siempre y cuando estas personas no estén capacitadas y sean capaces de diferenciar y concientizar de los problemas que pueden acarrear una manipulación errónea de la red.
* Realizar fuertes campañas de concientización con respecto a la ciberseguridad y la seguridad de la información. Instruir de forma periodica al personal con respecto a la importancia de una buena seguridad. Realizar ataque controlados durante el mes para ver si la capacitación brindada esta dando futos. Para obtener un resultado real es indispensable que nadie sepa del día ni la hora de ataque, ya que esto nos daría resultados negativos y el fin del ejercicio no serviría.
* Realizar un bloqueo mediante software de los puertos USB y que solo sean capas de leer información con la autorización de algún supervisor o del equipo técnico.
* Realizar una buena distribución de permisos de accesos y que una vez que ese personal quede desafectado de la empresa , esos permisos inmediatamente sean revocados.
* Algo muy importante es la entrega de equipos para el trabajo remoto. Realizar una formateo bit a bit para que el nuevo empleado no sea capas de levantar información sensible de la empresa. Por que hay que tener en cuenta quien fue el personal que utilizo ese ordenador antes y que puesto ocupaba dentro de la misma.
* Realizar backup de la información sensible de la empresa y mantenerla fuera del sistema ya que si en algún momento los activos se ven comprometidos por algún tipo de malware, este mismo sea incapaz de afectar a la copia de respaldo, esto permitirá aislar a el o los host infectados y luego de realizar una búsqueda de replicación del malware en el sistema , si todo es positivo poder levantar nuevamente y dejar todo funcionando.

Conclusión.

El mantenimiento de los sistemas como así también la capacitación del personal es optima para que un ecosistema funciones al cien por ciento. Estar siempre innovando con el hardware utilizado para tal fin es muy importante y entender que si la parte informática no va de la mano con el sector humano, es difícil que se pueda llegar a la excelencia en el trabajo.

‘QUIEN CONTROLA LOS DATOS, CONTROLA AL MUNDO’ Yuval Noah Harari.