DISEÑAR UNA NUEVA INFRAESTRUCTURA DE CIBERSEGURIDAD PARA UNA PYME.

Una Gestoría está reevaluando su actual estado de ciberseguridad, ya que recientemente han sufrido un ciber ataque , y en concreto un ransomware.

Deciden rápidamente ponerse en mano de profesionales, y es por ello que nos llaman para que evaluemos su seguridad informática, y podamos ayudarles para que no les vuelva a ocurrir de nuevo.

Realizando un primer análisis in-situ se detecta inmediatamente, que no existía ningún tipo de contramedida para poder parar este tipo de ataques; usuarios locales con permiso de administrador, USB conectados, gran información en los escritorios de los equipos, sistemas operativos obsoletos, aplicaciones pirateadas, sesiones de Windows sin estar bloqueadas, y sin estar el usuario delante, y en otros equipos vemos las password pegadas con posit en la pantalla.

Paralelamente otro compañero evalúa mediante un escaneo la IP publica de la empresa, y detecta que hay una gran exposición de la empresa (superficie de ataque) hacia internet. Tienen puertos abiertos como por ejemplo el RDP, pero también tienen un DNAT a un dispositivo NAS de trabajo que utiliza el puerto por defecto. Además, las contraseñas son débiles y sin estar actualizado el sistema operativo que utiliza el NAS.

Por otro lado, la web corporativa de la empresa tiene varios servicios vulnerables.

El cliente nos explica que su “amigo informático” en la época de la pandemia los “ayudo” para que pudieran teletrabajar, y les dejo puertos abiertos para poder teletrabajar (RDP). Sin duda, esto fue unos de los posibles motivos por los que la empresa sufrió el ciberataque.

Se observa que toda la información reside mayoritariamente en cada uno de los equipos locales, y que por suerte en el momento de ser ciber atacados (sábado por la tarde) solo un equipo se encontraba encendido. El empleado de ese equipo siempre dejaba el equipo encendido para poder teletrabajar, y además suele tener una copia de seguridad en su disco duro particular para poder llevarse la información cuando está en otros clientes y necesita acceder a su información reciente.

El CEO de la empresa quiere evitar que les vuela a ocurrir, y no sabe realmente por qué ha ocurrido.

Los han hablado de la “nube” (Cloud) cómo una buena alternativa para evitar este tipo de ataques…, pero desconoce si realmente les resultaría beneficioso para ellos económicamente hablando..., o si realmente pueden dejar todo tal y cómo está, y “confiar” en que no vuelvan a ser ciberatacados.

Nuestro trabajo como responsables de ciberseguridad será:

1) Hacer una auditoría técnica de carácter "gratuito" al cliente explicando que fallos de ciberseguridad se han encontrado en la empresa. Centrarse en los más evidentes.
2) Redactar un breve informe con el estado actual de la ciberseguridad en las empresas españolas para posteriormente comentarlo con el CEO.

   NOTA: Debe ser concreto y conciso, y fácil de entender por el CEO. Recordar que a un CEO estás cosas no le apasionan.

3) Explicarle en qué estado real se encuentra su empresa, y qué posibilidades tienen de volver a ser atacados.
4) Explicarle los "pro y contras" de montar toda su infraestructura en la nube. Contemplar diferentes proveedores de Cloud. Un análisis de costes.

   NOTA: No es necesario realizar un análisis super detallado, pero sin tener un coste aproximado, y una comparativa de precios.Realizar una pequeña simulación contemplando un NAS, Servidor, Firewall,etc..

Por último:

5) Diseñar una infraestructura de ciberseguridad en un laboratorio para los siguientes requerimientos:
   a. Bastionar a nivel microinformático todos los puestos utilizando; políticas de grupo, es decir, GPO para equipos y usuarios,etc...Un total de 10 equipo con sistemas operativos Windows 11

   b. Crear un nuevo sistema de almacenamiento central. Definir una estructura de permisos para los diferentes departamentos y usuarios.
   Departamentos: Contabilidad,Laboral,Nóminas, Herencias.
   usuario1….hasta usuario10.

      NOTA: Crear un convenio interno para dar de alta el nombre de equipos y de usuarios.

   c. Disponer de un sistema de alta redundancia en toda la empresa. Tanto a nivel de energía, discos duros, y datos de internet…

   d. Crear una red segmentada en la empresa con una red wifi para invitados, red de producción, y red de servidores.

   e. Implementar un sistema seguro para el teletrabajo, es decir, VPN, y MFA.

   f. Implementar un firewall de última generación. Reglas de firewall, crear políticas IDS e IPS para cada segmento de la red. Implementar políticas web, descifrado de Https, y fortificar al máximo dicho dispositivos.

g. Establecer medidas de seguridad para la web de la empresa. Sin contar con una posible revisión de código que llevaría a cabo el programador. Únicamente, defendiendo y hardenizando la web con nuestros medio y conocimientos.

h. Crear una estructura de domino con Windows Server. Hardenizar dicho sistema operativo para evitar ser atacado. Diseñar GPO diferenciadas para hardenizar los diferentes sistemas operativos de la empresa. Además, crear una GPO para las contraseñas de las empresas.

i. Montar un hypervisor hardenizado para albergar las diferentes VM: Aplicaciones de contabilidad, gestor documental, etc.. Con sistemas operativos Windows Server

j. Crear un plan de backup completo. Definiendo métricas (tiempo de copias y espacios)

NOTA: Se deja a elección del usuario "inventarse" los Gigas que puedan ocupar cada una de las máquinas, pero todo dentro de un cierto orden y lógica.

k. Diseñar un pequeño simulacro, y/o crear un BCP.
l. Diseñar planos de red y planes de backup de forma esquemática.
m. Analizar/estudiar que posibles sistemas de monitorización podría montarse.
n. Analizar/estudiar la recolección de log de los equipos Windows.
o. Recomendaciones a los empleados.
p. Sistema de protección contras sobre voltajes.