TRABAJO DE INVESTIGACIÓN: DISEÑANDO UNA RED

SISTEMAS INFORMÁTICOS
24-25

Trabajo de Alejandro Sainz Sainz

Alejandro Sainz Sainz

TABLA DE FIGURAS

INTRODUCCIÓN

En este trabajo nos vamos a dedicar a diseñar una red, más o menos para unas 20 o 30 personas. Para realizar esto nos vamos a centrar en detallar minuciosamente y paso a paso todos los aspectos, desde el comienzo, para llevar esta empresa a buen término. Cuando me refiero a esta empresa y todos sus pasos, hablamos de la selección de servidores, protocolos, medidas de seguridad, políticas de usuarios y otra serie de aspectos que intentaré detallar lo más posible, aunque quizá en algunos de ellos pasemos un tanto por encima, ya sea porque quizá reflejen un aspecto más secundario de esta tarea o, que también es muy posible, por falta de conocimientos sobre un determinado campo o por su dificultad para reflejarlos con mis propias palabras de una forma sencilla y fácilmente entendible.

Hay que tener en cuenta que intentaremos cubrir los pasos a diseñar y crear esta red, pero al no tener determinado el sector y gremio al que va a dirigida puede que algunos aspectos sólo se refieran como posibles o dependientes de que se cumpliesen una serie de condiciones. Estas pueden ir desde trabajadores móviles o deslocalizados, a aquellos que trabajan en remoto, la necesidad o no de servicios a través de una página web o si esta está simplemente pensada para darnos a conocer. Todas esas variables hacen que, de darse o no, tuviésemos la necesidad de implementar unas soluciones u otras, teniendo que dar información del cómo, el por qué y la manera en la que podrían ser relevantes estas cuestiones.

Intentaré también, de ser posible y relevante para el tema, ir enlazando todo con algunos otros de los temas que hemos ido viendo a lo largo de nuestra andadura, ya que algunas de estas cuestiones pueden volver a resultar útiles dentro de esta práctica y creo que podrían complementarla bastante bien.

Otro de los objetivos es reflejar la importancia sobre ciertas políticas, sobre todo en temas de seguridad ya que, a nivel empresarial, se ha convertido en un aspecto de máxima importancia, eso sí, siempre y cuando estén justificadas y no supongan un gasto y un despliegue superficial y sin sentido alguno. Hay que tratar siempre que cada acción importe y sume, de que cada funcionalidad en una red tenga un propósito, ya que en sistemas que quizá puedan ser muy limitados o que se necesite que sean más escuetos, habrá funcionalidades que no aporten y que sean más un lastre o un ligero impedimento.

Ahora ya, sin nada más que añadir, vamos a comenzar con este trabajo.

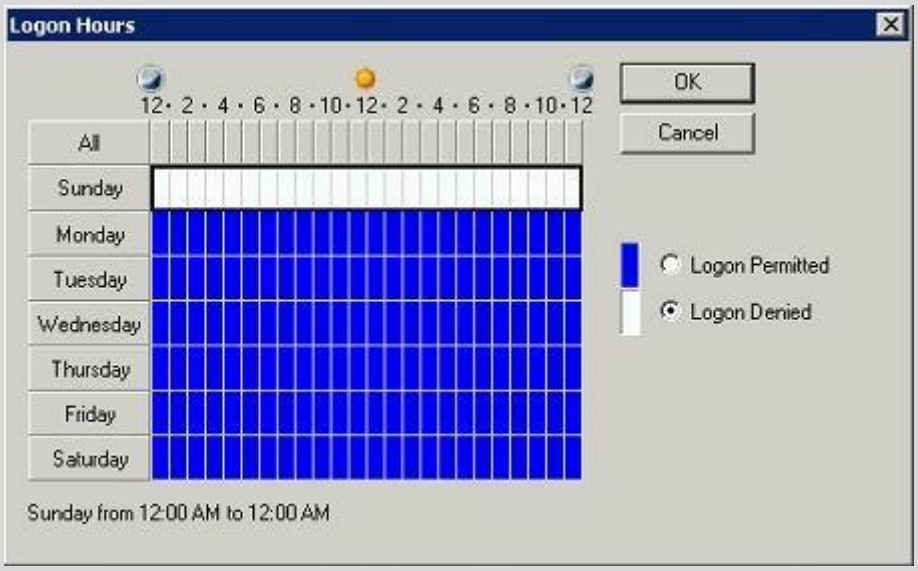
USUARIOS, DIRECTIVA, PERFILES Y SEGURIDAD

Lo primero que voy a comentar aquí, que me parece básico y que es lo primero a tener en cuenta, es que esta me parece la parte más frágil de la cadena y doy mis motivos.

Podemos tener la mejor seguridad del mundo, firewall y servidores cuánticos, routers con 100 capas de seguridad y políticas extremadamente seguras y complejas, que incluso con todos eso, un usuario va a conseguir, y de seguro de forma involuntaria, encontrar más vulnerabilidades y fallos que muchos técnicos en seguridad. Y eso no es de chiste, es que yo también en alguno de mis trabajos, he sido un usuario de sistema y me he tropezado con casos en los que sabiendo lo que hacía, y otros de forma involuntarias, acabas tocando algo que casca el sistema.

¿Por qué digo esto? Fácil, para justificar el motivo que me impulsa a escribir lo que viene a continuación.

Las políticas en torno a los usuarios, su interacción con el sistema y la libertad que tengan durante su uso, salvo en casos especiales que se necesite otra cosa, deben de ser lo más restrictivas posibles.



1 GESTOR DE HORARIOS DE ACTIVE DIRECTORY

https://www.manageengine.com/latam/active-directory-audit/kb/how-to/como-configurar-las-horas-de-inicio-de-sesion-en-active-directory.html

A que me refiero con más restrictivas. A qué se deben de limitar lo más posible las acciones de los usuarios para evitar esos problemas que puedan surgir.

Como vemos en la imagen anterior (Gestor de horarios de conexión de Active Directory) podemos incluso limitar las horas en las que un equipo, ya sea identificado por IP o MAC, se conecta contra el servidor, es decir, comienza su sesión identificándose en el server.

Ahora bien, lo que estamos trabajando aquí es una empresa ficticia, de unas 30 personas, de la cual no sabemos su actividad ni el régimen de funcionamiento que tiene. Así que vamos a comenzar desde el principio intentando evaluar todas las opciones posibles.

Como tipos de perfil de usuario yo siempre optaría por perfiles obligatorios, que no puedan ser modificados por los usuarios. A estos se les van a asignar zonas de almacenamiento que posiblemente no estén ubicadas físicamente en su equipo, así que lo que no vamos a dejar es que modifiquen bajo ningún concepto el perfil de usuario. Ahora bien, existen tipos de actividad y departamentos o tareas que requieran de ciertas modificaciones las cuales no podemos permitir que el grupo de IT, en caso de que lo haya, esté pendiente de hacerlas cada vez que un usuario lo necesite. Imaginemos que nos dedicamos al desarrollo, como en el módulo que estudiamos. Descargar plugins, IDEs, dependencias y un largo etcétera. Vamos a tener que permitir que los usuarios modifiquen su sesión, sus archivos, que toquen su almacenamiento. No podemos tener perfiles obligatorios para ellos, ya que su actividad puede requerir de muchos cambios que no podemos modificar cada dos por tres. Por otra parte, en casos en el que sean trabajos más repetitivos y estáticos podemos hacer el perfil totalmente inmutable.

Luego siempre hay que tener en cuenta que quizá una empresa pueda contar con trabajadores que se muevan, comerciales, vendedores, servicios técnicos a otras empresas, personas que realizan su trabajo en remoto por el motivo que sea. En esos casos es más que seguro que deberemos tener la posibilidad de habilitar perfiles móviles, que puedan ser ejecutados en diferentes dispositivos y quizá con una libertad de horarios mucho más amplia.

2 HAY ALGUNOS QUE EL TELETRABAJO LO LLEVAN A OTRO NIVEL

https://images.ecestaticos.com/hNzgpu-pQQs-Tm8_Ksu3R3RVDdk=/0x0:1000x750/996x747/filters:fill(white):format(jpg)/f.elconfidencial.com%2Foriginal%2F8d5%2Fa6b%2F4d1%2F8d5a6b4d1ca972753ff6e55729dfe37c.jpg

Todo va a depender de los tipos de actividad que llevemos a cabo en nuestra empresa. Luego de seguro tendremos perfiles especiales, ya sean jefes u otro tipo de cargos, con los que habrá que tener más manga ancha.

Pero, en conclusión, yo por mi parte, restrictivo a más no poder, siempre que eso no interfiera con la naturaleza propia de nuestra actividad.

Después de esto, si hablamos de permisos, de nuevo hay que ser restrictivo. Cada perfil de usuario debe de ir asociado a un grupo, dependiendo del departamento y dentro de su actividad en el mismo. Pueden existir trabajadores que, dentro de un departamento en concreto, tengan ciertas atribuciones o responsabilidades que requieran de permisos distintos con respecto a determinados archivos o recursos. Intentaremos siempre que los permisos de ejecución y de escritura estén perfectamente acotados a un directorio, un grupo de ficheros o un recurso en concreto, eliminando estos permisos del resto del sistema, para que no puedan interferir con otros grupos y sus recursos asociados ni con aquellas partes propias del sistema que sólo deberían de ser manipuladas por el departamento de TI.

Por poner algún ejemplo en concreto, aunque va a quedar algo vago, podríamos tener un departamento de desarrollo cuyos permisos van a estar localizados en los archivos compartidos o en la parte de almacenamiento propio de ese departamento. Allí pueden crear sus propios archivos, editarlos y ejecutarlos. Por el contrario, perderán esos permisos en otras zonas del sistema, en aquellas pertenecientes o propias de otros departamentos. No deberán de tener posibilidad de escritura y ejecución en zonas como por ejemplo Marketing, o ventas, ya ni hablar de dirección o recursos humanos. Y sólo deberían de tener permisos de lectura en ciertas zonas o archivos que no supongan un riesgo o cuya lectura no suponga ningún problema.

Evidentemente el único grupo que debe de tener acceso a todos estos permisos son los técnicos, aunque también deben de tener sus limitaciones. A nadie le gustaría que, mientras realizan tareas de mantenimiento, borren archivos propios de otro usuario. Por lo tanto, no deberían de poder modificar esos archivos. Moverlos quizá, leerlos por su puesto, sobre todo por el hecho de que puedan necesitar verificar el contenido de algunos archivos.

En conclusión, mediante el uso correcto de permisos y de almacenaje compartidos, debemos acotar de forma precisa el ámbito de actuación de cada grupo y cada usuario dentro del propio sistema, dándole cierta libertad sólo en ciertas zonas y en lo referente a recursos propios y que son imprescindibles para su trabajo. En el resto de las zonas o secciones, las acciones de ese usuario no deberían de tener ningún impacto. Cada grupo o usuario sólo debe de ser consciente de su propia actividad y de aquellas que estén relacionadas con él, del resto, si no es consciente, mucho mejor. Y es con esa mentalidad con la que creo que debemos de preparar los permisos y los perfiles.

POLÍTICAS DE CONTRASEÑAS Y CONTRASEÑAS

En cuanto a contraseñas tendremos que exigir unos mínimos de longitud y complejidad. Que se deban de cambiar con regularidad, cada dos o tres meses, pero sin ser molesto. Con un máximo de intentos erróneos de conexión, entre tres y cinco me parece un buen número.

Luego ya todo está en manos de los usuarios. Donde apuntan o guardan sus contraseñas, si las comparten o no, si usan las mismas dos o tres contraseñas en bucle cada vez que toca modificarlas. A este tipo de cosas también me refería al hablar del eslabón más débil de la cadena.

Con las contraseñas puede pasar cualquier cosa. Que la tengas en un post-it pegada a la pantalla del ordenador, que uses 1234 y al siguiente cambio sea 4321, que un día, que a todos nos puede pasar, te obceques o te ofusques y rebases el número máximo de intentos permitidos simplemente porque colocaste mal los dedos en el teclado o porque te confundiste con la contraseña que utilizabas el mes pasado.

3 USANDO CONTRASEÑAS SEGURAS

https://www3.gobiernodecanarias.org/educacion/cau_ce/servicios/web/sites/www3.gobiernodecanarias.org.educacion.cau_ce.servicios.web/files/inline-images/img1_conlogo.png

En cuanto al resto de políticas de las cuentas, otra vez lo mismo. Hay que intentar ser restrictivo, en la medida de lo posible. Suena a tirano, pero eso ayuda a prevenir cierto tipo de errores y de situaciones que en un ámbito empresarial y de trabajo pueden ser molestas y su resolución se puede convertir en un dolor de cabeza.

Una vez un trabajador cesa su actividad en la empresa, ya sea de forma permanente o temporal, la medida mínima es deshabilitar su cuenta, luego en determinados casos lo más seguro y lo propio será eliminar de forma permanente esa cuenta y ese perfil de usuario.

En cuanto a las auditorías de seguridad y de sistema, hablando de las experiencias propias en otras empresas, no he visto tantas ni con tanta asiduidad. Pero bien es cierto que deben de ser realizadas, aunque en mi opinión, si tenemos un buen sistema de logs, un buen sistema de seguimiento y la monitorización de eventos podemos espaciar más las auditorias de seguridad, quizá cada año y medio y dos años. Todo ello depende de que bien hayamos preparado todo en un inicio. De todas formas el uso diario de los sistemas hará que vayan apareciendo nuevas situaciones o problemáticas, además de que se tendrán que realizar actualizaciones de software e incluso hardware que puedan cambiar las dinámicas de nuestro trabajo y el funcionamiento de nuestro sistema, por lo que en esos momentos tendremos que realizar nuevas auditorías de seguridad para verificar que los cambios no dan lugar a nuevos problemas o brechas de seguridad que puedan suponer problemas a posteriori o traer de vuelta problemas que considerábamos resueltos.

En este apartado lo que considero más básico es el sentido común para todo y el no querer obviar aspectos que, por obtener una mayor comodidad o flexibilidad, a la larga nos supongan un problema y una carga extra de trabajo que nos podemos ahorrar con unas buenas prácticas básicas. Con esto me refiero a no exigir una determinada complejidad en las contraseñas por hacerlo más fácil a los usuarios, o que sólo se les solicite cambiarlas un mínimo número de veces al año, véase 1 o 2. A veces se nos puede hacer tedioso el tener que llevar a cabo estas tareas que se nos hacen molestas, pero que a la larga pueden hacer nuestro día a día más llevadero y seguro en el ámbito del trabajo.

Hay que tener en cuenta en todo esto que somos como somos, por comodidad somos incapaces de pasar un pequeño espacio de tiempo aprendiendo algo nuevo o realizando una pequeña tarea que no nos supone mucho esfuerzo. Pero en este caso, con estas normas hay que intentar ser lo más estricto posible.

SERVIDORES

Esta es una pregunta a la que creo que no sabría dar una respuesta concreta.

¿Es correcto usar un servidor DHCP que nos de servicio al resto de equipos? Si, completamente. Eso nos liberaría de tener que configurar manualmente cada uno de nuestros dispositivos y este servidor se encargaría de proporcionarles una dirección IP de forma automática por nosotros. Pero, por el contrario, configurar manualmente cada una de las direcciones dentro de nuestra infraestructura, aprovechando que hablamos de alrededor de 25-30 equipos y no deberíamos de tardar mucho, nos permite mucho contralar el sistema. Es decir, si me aseguro de que cada equipo tiene una IP fija puedo tener mi red fiscalizada todo el tiempo. Me explico, si se de forma segura que un equipo que es usado de forma única por un usuario tiene siempre la misma IP, puedo tener identificada su actividad, sus logs de incidencias, etcétera… de una forma mucho más rápida. Por el contrario, al tener habilitado un servidor DHCP, las posibles direcciones se van permutando de un día a otro, por lo que, aún siendo relativamente simple, para identificar el tráfico o la actividad voy a tener que realizar un trabajo extra a la hora de controlar la actividad de cada uno de mis usuarios o de cada una de mis estaciones. Es cierto que las credenciales al logearse contra un servidor ayudan a reducir mucho esa tarea extra, pero mantener las IP fijas asignadas a una estación concreta hace que se la pueda identificar mucho más rápido. Luego está la parte de que, usando el sistema de asignación fijo, puedo asignar rangos según departamentos, lo que me hace más fácil el trabajo a la hora de aislar segmentos de red. Por ejemplo podría aislar un departamento entero en caso de que lo necesitase limitando un rango determinado de IP, pues sé que un solo departamento está ubicado en un rango concreto, mientras que si usamos un servidor DHCP debo hacerlo manualmente una por una después de identificar cuáles son las direcciones que se han asignado a ese departamento en el momento determinado que lo necesite. Sin embargo DHCP nos ofrece algunos aspectos mejores a la hora de resolver conflictos. Sabemos que es mucho más difícil que se produzca un conflicto, pues el servidor no va a designar una IP ya asignada a otro equipo, mientras que en estático debemos tener un cuidado extra para que no se produzcan estos errores. Además de esto, ante algunos problemas en estático son más difíciles de identificar y en DHCP con algunos comandos (renew, etc) es más fácil de obtener una solución momentánea o permanente para solventar problemas.

Cada aspecto tiene sus pros y sus contras, supongo que es cuestión de elegir cual es el que creemos que nos puede venir mejor dependiendo de la situación.

¿Servidores de aplicación? Evidentemente este servidor si depende de la actividad de nuestra empresa. ¿Usamos una suite de gestión?¿Movemos grandes cantidades de datos e información?¿Aunque pudiésemos ejecutarla en local podemos mejorar mucho el rendimiento de nuestra empresa o negocio dejando que un servidor proporcione el entorno de la aplicación y gestiones las conexiones de los usuarios desde sus estaciones?

Estas son sólo algunas de las preguntas que debemos plantearnos a la hora de decidir si vamos a utilizar un servidor de aplicación en nuestra organización. Y lo malo es que no hay una sola respuesta válida. La naturaleza de nuestra actividad va a determinar si lo necesitamos o no. Y lo complicado es que dentro de esta sección podríamos incluir el servidor de base de datos. ¿Qué tan grande es el volumen de información que manejamos?¿Realizamos muchas transacciones de datos al día?¿Todos nuestros empleados trabajan contra la base de datos o sólo algunos?¿Trabajan permanentemente contra la base de datos o sólo de forma parcial? De nuevo debemos de valorar nuestras necesidades.

Ya sé que parece que digo mucho sin decir nada. Pero el problema es que cada empresa y cada actividad va a tener unas necesidades distintas.

Por poner un ejemplo, yo trabajé en una Mutua de Accidentes de Trabajo. Lleva datos de todos los empleados y empresas asociadas, por lo tanto un servidor de base de datos no era opcional, era una necesidad en imperativo. Además de que al conectarse contra los servidores de la Seguridad Social se debían de poder consultar los datos de trabajadores no afiliados. Todavía más necesario. Ahora bien, imaginemos una asesoría. Trabaja también con trabajadores y empresas, pero quizá no necesite un servidor de base de datos, pues ellos sólo trabajan con los datos de aquellos que les competen, así que su volumen no es tan alto. Tendrán una BD, posiblemente sí. ¿Necesitan un servidor dedicado de datos? En algunos casos seguro que no.

Entonces ahora tendríamos que pensar cual es la necesidad de nuestra empresa.

Veamos un servidor de archivos y de impresión ahora. Es algo que siempre es útil, aunque quizá el de impresión va perdiendo fuerza últimamente. Todo el tráfico suele ir por la red y se ha reducido bastante la cantidad de papel que se necesita. Aún así, si no queremos tener varias impresoras asociadas a varios equipos, con un servidor de impresión y sólo un par de dispositivos ya podemos tener cubierta una empresa del tamaña al que nos estamos refiriendo. Así que siempre es una buena opción. Por la parte de archivos, a mi entender siempre es útil poder tener los archivos en un servidor, ya sea FTP o de otro tipo. Suele ser muy útil tener los archivos centralizados sobre todo a la hora de gestionar copias de seguridad de esos archivos y de protegerlos. Además hay que tener en cuenta que si guardamos los archivos en las estaciones de trabajo y estas dejan de funcionar o se desconectan de la red, la información en ese equipo deja de ser accesible para otros usuarios de la red e incluso, el propio usuario de ese equipo. Así

que en mi opinión es una opción más que recomendable independientemente de la actividad que desarrollemos, siempre y cuando esa actividad tenga que ver con información y datos.

Servidores Web, DNS y de Correo. La web marca el camino, así que el servidor web creo que es casi un imperativo hoy día, ya sea un servidor propio, uno en la nube o que lo contratemos en una plataforma que lo aloje. Lo vamos a necesitar sí o sí. La gran mayoría de empresas cuentan con un sitio web para darse a conocer, para gestionar compras y ventas, reservas, etcétera… Hoy día raro es quien no tiene uno. Y evidentemente, buscaremos que sea seguro y trataremos de adecuarnos al protocolo HTTPS. Existiendo este no creo que tenga sentido seguir usando solamente HTTP.

El servidor DNS directamente creo que no. Existen los de Google, cloudflare y un largo etcétera… Si nosotros tuviésemos el nuestro propio sería mucho más lento y menos fiable. Si la empresa fuese más grande, con diferentes sedes y multitud de equipos o de diferentes servidores lo podríamos pensar, pero con los números que estamos trabajando yo creo que no.

Y por último el servidor de correo. ¿Cuánto tráfico entrante/saliente tenemos de este tipo? Lo vamos a usar sólo para comunicación interna dentro de la empresa? ¿O todos los trabajadores necesitan un servicio que les permita enviar y recibir del exterior? Si este último caso es afirmativo, si, deberemos de configurar uno. ¿Por qué? Por la sencilla razón de economizar recursos. Sustituimos los gestores de correo locales por uno centralizado ya preparado para esa tarea y para filtrar remitentes y destinatarios mediante una sola máquina y conexión. Debemos de valorar cuales son nuestras necesidades.

MEDIDAS DE SEGURIDAD EN RED

Suena un poco irreflexivo comparado con lo anterior, pero la respuesta es sí, a ojos ciegos. ¿A que me refiero? A que más grandes o pequeñas, pero debemos de pensar en la seguridad en la red. Así que muchas veces antes de pensar en las que vamos a usar debemos simplemente decir sí, quiero medidas de seguridad ante la red.

¿Cortafuegos? Por supuesto. Más grande, menos, con blacklist o sin ella, con posibilidad de admitir conexiones VPN externas para trabajadores en remoto o con movilidad, con capacidad propia de filtrar y observar el tráfico o no, pero hay que tener uno. Si vas a comprar una casa la compras con una puerta, pues en este caso lo mismo. Si vas a trabajar junto a la red, esta es tu puerta. Será más grande o menos, más robusta o menos, pero tienes que tener una

puerta. Esto es un impepinable. Luego habrá que decidir todos los extras que traiga o no, pero no existe el no en cuanto a la decisión de tener un cortafuegos cuando vas a trabajar hacía la red. Aunque sólo tengas uno pequeño es mejor que no tener nada.

¿Vamos a usar cifrado? Ya sea en mayor o menor medida, sí. La información es muy importante, nuestros datos, los de nuestros clientes, nuestros proyectos. Luego dependerá de la importancia de los datos con los que trabajemos si necesitaremos doble, triple, hashing, encriptado. Y luego posiblemente en nuestros servidores internos, para salvaguardar esos datos una capa de cifrado no le hace daño a nadie. Que es un poco más lento porque debemos desencriptar y porque los datos cifrados llevan una capa extra de información que hay que retirar a la hora de trabajar con ellos, es cierto. Que es más difícil para la gente de pocos escrúpulos retirar esa capa de información y que a nosotros nos permite dormir mejor, también es cierto. Así que un poquito de cifrado por aquí y por allá no nos va a hacer ningún daño. Además teniendo en cuenta que hay mucha gente al acecho escondida en la red, dentro de los servidores DNS, en páginas de dudosa legalidad, en wifis gratuitas simulando ser inocuas. No seremos los reyes de la criptografía, pero tampoco vamos a desdeñar unas herramientas que nos pueden alegrar el día. Si el cortafuegos es la puerta, esta es la cerradura. Compra una buena y ten una buena llave. No te puedes arrepentir.

DMZ. Esta es la única que considero opcional. Si tu sitio web va a recibir mucha atención y mucho tráfico, sin duda. Vamos a aislarnos un poco de ese tráfico y vamos a obtener otra capa de protección. Sin embargo si nuestro volumen de visitar es pequeño, si sólo disponemos de una página de información en la que la forma de interactuar es mínima, no creo que tengamos mucha necesidad de una zona desmilitarizada. Si además nuestra forma principal de comunicarnos es mediante el correo u otro tipo de plataforma y no por nuestra web, es decir, nuestra forma de interactuar no es principalmente por la web, creo que este es un elemento que podemos obviar sin que suponga un problema, al contrario que los dos anteriores, que van a ser necesarios sí o sí en mayor o menor medida.

En cuanto a la seguridad física, en el caso en el que nos encontramos, con el tamaño de empresa al que nos referimos, debemos de centrarnos en el servidor. Ya que él va a centralizar gran parte de los servicios, las medidas físicas deben de ser para él. Control de acceso, vigilancia y monitoreo. Es nuestra pieza central, y es una pieza que una vez perdida es difícil de recuperar. Así que unos mínimos debemos de tener siempre. Como mínimo el control de acceso. Estar en una sala en la que no pueda entrar cualquiera y que se tenga un listado de quien y cuando accede ya es una buena implementación en este sentido. Además podemos contar aquí con los ya vistos sistemas raid, que son a la vez un sistema físico y lógico de seguridad. Ya que nos permiten salvaguardar nuestra información en caso de avería, ataque o catástrofe de otra índole.

MONITORIZACIÓN

En este aspecto tenemos una amplia variedad de herramientas que podemos usar.

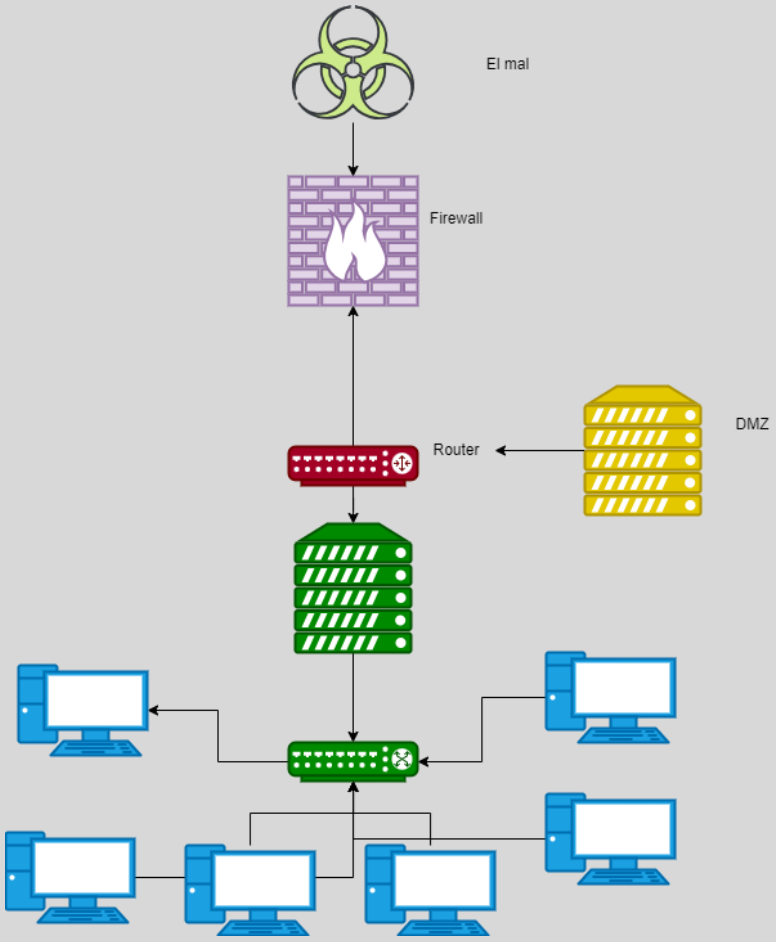
Siendo nuestra empresa pequeña podríamos usar opnsense o pfsense. Vamos a decir que son herramientas híbridas que nos hacen las veces de cortafuegos y herramienta de monitorización que nos ayudan a tener protección en tiempo real y a monitorizar las conexiones entrantes y salientes además de la situación del tráfico.

Y si nos vamos a casos más grandes, el mercado nos surte de una gran cantidad de herramientas profesionales con resultados probados durante mucho tiempo. Entre sus características las podemos tener con monitoreo en tiempo real, con alertas personalizadas diferenciando entre alertas de tráfico o de amenazas, de rendimiento de la red e incluso de optimización del tráfico y de los cuellos de botella que se puedan producir.

Aquí podemos elegir entre una amplia variedad dependiendo de nuestras necesidades.

Desde las ya nombradas OpnSense, OpfSense a otras como WireShark, Nagios, SolarWinds. Aquí ya va a depender de cuanto tráfico manejemos, de la cantidad de conexiones entrantes entre las cuales se pueden esconder intentos de conexión de honestidad dudosa. En todo ello deberíamos decidir según nuestra necesidad.

CENTRANDONOS EN NUESTRO EJEMPLO



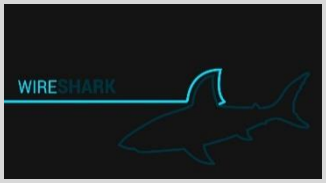
4 PEQUEÑO EJEMPLO ORIENTATIVO

A partir de este punto, como además ya creo que he divagado y viajado mucho a lo largo de las posibles opciones que tenemos, voy a intentar dar una idea concreta de lo que utilizaría yo de entre todo lo que he explicado anteriormente intentando enfocarme en el ejemplo que se nos ha proporcionado.

Con el diagrama anterior, que se ha realizado con draw.io aunque de forma más vaga y orientativa, ya que no representa completamente el caso que se nos dio, voy a intentar explicar ligeramente lo que yo haría. Como vemos en la imagen tenemos al mal intentando entrar en nuestra casa, así que lo primero es construir una buena puerta, con un firewall medianamente decente. Dado que no es una empresa relativamente grande y posiblemente este comenzando yo trataría de utilizar una máquina dedicada para hacer de firewall y de monitorización a la vez.

Para ello usaría OpnSense y WireShark, como cortafuegos y monitorización conjuntas.

5 Logo de OpnSense



6 El tiburón nos vigila.

Creo que con estas dos herramientas ya podríamos tener una buena capa de protección de inicio. Además siendo open source sólo debemos de preocuparnos del coste de la máquina en si misma.

En el diagrama incluyo una zona DMZ. Está ahí porque es una opción, pero ya que estudiamos lo que estudiamos, voy a optar por decidir que nuestra empresa va a ser de desarrollo y programación. No vamos a tener una página en la que vendamos productos ni regalemos viajes al Caribe, así que finalmente, sólo la he puesto para que quede todo reflejado, yo en este supuesto no la usaría ni le daría recursos para ella. No creo que nos sea necesaria, que no quiere decir que no sea útil. Siempre va a tener utilidad pero no en nuestro caso. No me parece una prioridad.

Luego tendremos nuestro router, que nos hará las veces de Gateway, para dar salida al exterior a toda nuestra infraestructura. Aunque en el diagrama el cortafuegos está puesto al frente es más simbólico que otra cosa, por el hecho de haberlo comparado con la puerta. El cortafuegos le colocaríamos entre el router y nuestra red, filtrando entradas y salidas y todas las conexiones que se produzcan y monitorizando todo el tráfico.

Luego tenemos nuestro servidor. Yo en él, dada la naturaleza de la empresa, colocaría el servidor de archivos, el servidor web y el de correo. A ser posible virtualizados cada uno por separado y divididos en contenedores independientes, para no llamar a la tragedia y que todo se vaya al garete en un momento. Siendo desarrolladores podríamos contar con un servidor de BD pero creo que no es nuestra finalidad, nosotros desarrollamos las bases de datos, creo que serán otros los que tengan que alojarlas. También en el instalaríamos el controlador de dominio, que sería un Active Directory. Ya sé que normalmente yo soy más alternativo y de buscar soluciones con forma de pingüino, pero por una vez vamos a fiarnos de Microsoft.

Las estaciones de trabajo tendrían IP estática, quiero controlar yo la IP de cada uno, y aunque he sido muy vehemente con los perfiles obligatorios, siendo desarrolladores creo que tendría que optar más por perfiles locales en cada máquina, pues cada desarrollador podría tener que utilizar diferentes herramientas dependiendo de su ámbito, front, back, BD, etcétera… Eso sí, las políticas de seguridad bien restrictivas ya sean las contraseñas, los espacios de almacenamientos, las horas a las que se pueden conectar y las credenciales personales. Sólo

sería ligeramente flexible con perfiles móviles en caso de teletrabajo o que existiese algún departamento comercial. Mucho cuidado también con esos de decidir instalarse cualquier plugin o extensión, hay que controlarlo todo. Y no voy a entrar ni a mencionar ni a valorar los perfiles de invitado. Si yo viese a alguien usando este tipo de perfil, lo primero que hago es sospechas y luego… ya veremos.

En cuanto a la estructura de la red, creo que con un switch nos valdría. Con uno lo suficientemente grande de 32 puertos en el caso de que trabajemos en una sola planta. De no ser así habría que usar varios dispositivos. Si tuviésemos la necesidad de varios dispositivos tendríamos que segmentar la red por cada departamento. En caso de sólo necesitar uno la podríamos segmentar mediante el uso de VLANS, que aunque es más complicado puede sernos de gran utilidad.

CONCLUSIÓN Y REFLEXIÓN

En esta pequeña práctica, aunque ficticia, hemos visto, y seguiremos viendo en un futuro si nos encontramos con algo parecido, de lo delicada y minuciosa que puede llegar a ser desarrollar una red. En este caso, dado que nos centrábamos en una red pequeña, nos hemos tenido que plantear gran cantidad de cuestiones, buscar las respuestas y, como ya he mencionado en otros trabajos, navegar por inmensos agujeros negros de información, conocimiento y especificaciones técnicas relativas a todo este ámbito.

Desde elegir una topología de red hasta definir políticas de seguridad, nos damos cuenta de que cada parte de todo el proceso puede ser crítica, puesto que la elección, independientemente de que sea la más o menos optima, de cualquier variable puede afectar a todas las demás.

Podríamos diseñar un complejo sistema que funcione como un reloj, pero en caso de no ser escalable y encontrarnos luego con esa necesidad hace que ya no nos sirva para nuestro propósito. La elección de un sistema operativo o una serie de aplicaciones cuyo soporte no es bueno o no es de una duración larga y que cubra nuestras expectativas puede llevarnos a tener que cambiarlo todo en poco tiempo, lo que de nuevo puede invalidar nuestras elecciones.

Cosas como esta nos dan una idea de lo frágiles que pueden ser estos sistemas ante los cambios y que de forma permanente tendremos que trabajar sobre el mismo, modificando, mejorando y actualizando todo nuestro sistema.

Este pequeño caso, aunque no hayamos entrado en detalles muy concretos y técnicos, nos da una idea de lo titánico y masivo que se puede volver cuando se diseñan redes muy grandes, del tipo MAN o superiores. La cantidad de variables que entran en juego y que hay que tener en cuenta son muchas: segmentar una red, uso de VPNs, tipos de firewalls, como configurarlos, el hardware necesario y un largo etcétera de otras preguntas y variables.

BIBLIOGRAFIA Y ENLACES

https://smalltec.es/dmz/

https://isnum.com/glosario-ciberseguridad/vlan/

https://www.ionos.es/digitalguide/servidores/know-how/broadcast/

https://www.ionos.es/digitalguide/servidores/know-how/broadcast/

https://isnum.com/glosario-ciberseguridad/vpn/

https://keepcoding.io/blog/que-es-pfsense/

https://wiki.oasixcloud.es/Iaas/VirtualDataCenter/Network/VRouters/OPNSense

https://learn.microsoft.com/es-es/windows/win32/shell/about-user-profiles

https://www.manageengine.com/latam/active-directory-audit/kb/how-to/como-configurar-las-horas-de-inicio-de-sesion-en-active-directory.html

https://learn.microsoft.com/es-es/dotnet/framework/wcf/feature-details/auditing-security-events

https://www.paessler.com/es/it-explained/server

https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

https://www.supermonitoring.es/blog/herramientas-de-monitorizacion-de-redes/