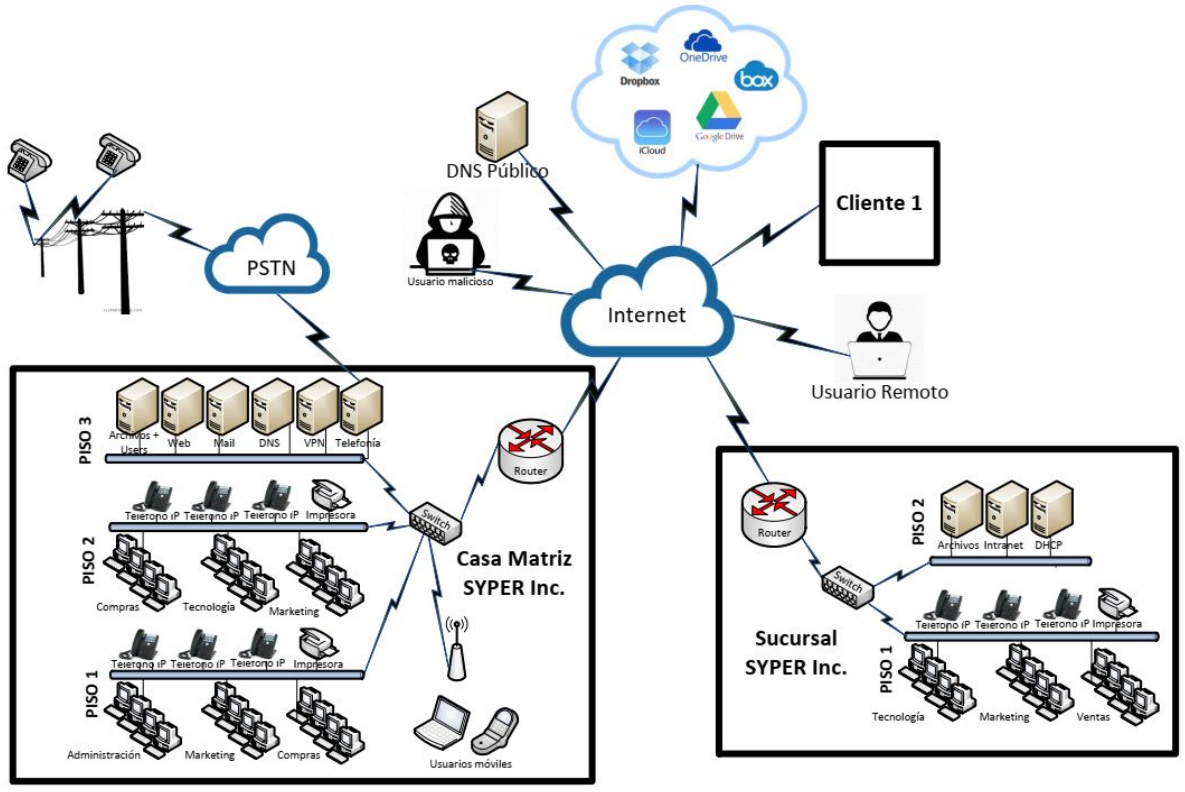
Seguridad y Privacidad en Redes.
Ejercicio integrador:
Consultor Senior en Seguridad



Integrantes:

Apellido y Nombre	Legajo
Duran, Paula Mariel	
Canales, Lautaro Daniel	

Análisis de la topología

Actualmente en la topología tanto en Casa Matriz como en Sucursal se conecta desde un mismo switch hacia todos los pisos, sin diferenciar entre servidores, hosts, dispositivos móviles, impresoras o teléfonos IP.

También desde sucursal se deben compartir servicios de casa matriz y se desconoce el tipo de conexión existente. Se puede suponer que existe algún tipo de conexión VPN, ya que existe un único servidor DNS en Casa Matriz, y es el que debe resolver las peticiones DNS de toda la organización, así como también existe un único servidor de DHCP, de Intranet, Telefonía y VPN, que deberían poder ser accedidos tanto desde Casa Matriz como desde Sucursal, y no desde internet.

Recomendaciones

Es recomendable crear zonas desmilitarizadas (DMZ) para los servidores a través de Firewalls de red, de esta forma se puede restringir el acceso y uso indebido de los mismos, tanto desde fuera de la organización como desde dentro.

Sería óptimo cambiar los dispositivos de red actuales (un solo switch) por redes privadas para cada área, con un router o en su defecto por virtual lans a través de un switch de capa 3. De esa forma debería quedar una subred para Tecnología, una para Compras, una para Marketing, una para Administración, una para Ventas, una para los servidores, una para los teléfonos, y por último, una conectada directamente hacia el router de borde para los usuarios móviles.

Respecto a la red de telefonía, se debe encontrar separada de la red de comunicación entre ordenadores, ya que sólo se dedican a comunicarse entre ellos, y con su servidor para poder salir a la red PSTN.

Con estas modificaciones se puede asegurar que cada usuario sólo tiene acceso a los recursos que le competen a su área a través de estas subredes, y, con las restricciones correspondientes del Firewall, se puede asegurar que entre redes no se comuniquen directamente dos hosts.

En el caso de las impresoras, se deja la libertad de comunicación con la que corresponde a cada piso.

Se recomienda, además, utilizar el sistema de usuarios y grupos para asignar la subred correspondiente a los usuarios remotos.

Para la comunicación entre Sucursal y Casa Matriz, se recomienda una nueva conexión física dedicada a ello, utilizando VPN como forma segura de comunicación, y teniendo como alternativa, la conexión física a internet en caso de algún problema con la dedicada a VPN.

Al mismo tiempo se aconseja, de ser posible, que ambas conexiones pertenezcan a distintos ISP (Proveedores de Servicio de Internet), ya que, de ésta forma, se puede asegurar la comunicación entre Sucursal y Casa Matriz si alguno de estos proveedores no pudiera brindar servicio momentáneamente.

Dado el uso de las redes VPN para usuarios remotos, se considera oportuno que, dependiendo el usuario, se conecte a una red VPN-área-usuario, y así se pueda acceder a todos los contenidos que le correspondan, pudiendo identificar fácilmente que está conectado de manera remota.

Acerca de los servicios que se prestan desde SYPER Inc.

Actualmente, los detalles de los servicios que se prestan tanto internamente como externamente desde SYPER Inc, son lo siguientes:

- **DNS**: Tiene alojada la zona *syper.local*. Es el servidor primario de dicha zona la cual es una zona interna no consultable desde internet. Todos los equipos de la red interna (tanto de Casa Matriz como de Sucursal), tienen configurado este equipo para la resolución de nombres. Todos los nombres que desconoce, los reenvía a un servidor ubicado en internet (DNS Público).
- **Archivos + Users:** Guarda los archivos compartidos de los usuarios de SYPER Inc. A su vez es donde se encuentran definidas las cuentas de usuarios de los 500 empleados de la compañía.
- **Web:** Aloja la página pública de la empresa accesible desde internet a través de la dirección *http://www.syper.publica*. Además, contiene también otras aplicaciones corporativas entre las que se destacan:
    - Liquidador de sueldos
    - Localizador de internos telefónicos
    - Webmail interno (*http://webmail.syper.local*).
- **Mail:** Servicio de correo de la empresa (*mail.syper.local*).
- **VPN:** Posee las políticas para el acceso desde la red pública a la red interna.
- **Telefonía:** Es el servidor de telefonía IP de la red. Es además el nexo con la red PSTN.
- **Archivos:** Guarda los archivos compartidos de los usuarios de Sucursal
- **Intranet:** Posee la página de la intranet de la empresa. Se accede a través de *intranet.syper.local*.
- **DHCP:** Dado que no tenemos una descripción exacta de qué tipo de servicio DHCP brinda éste servidor, asumimos que configura todos los hosts de la organización, incluidos aquellos que se conecten de forma remota.

Recomendaciones para maximizar la disponibilidad de los mismos.

Dado que actualmente existe un único servidor por cada recurso necesario en un edificio (DNS, DHCP, VPN, Users, Telefonía) para toda la organización, se recomienda fuertemente, para asegurar la disponibilidad de estos servicios, y disminuir los tiempos de respuesta entre requerimientos, tener uno de cada uno de ellos en Casa Matriz y otro en Sucursal.

Idealmente los servidores DNS y Users deben estar espejados, de forma tal que, en caso de que se modifique alguno de ellos, estos cambios se vean inmediatamente actualizados en el correspondiente al otro edificio.

Los servidores DHCP y Telefonía de cada edificio deben estar configurados sólamente para atender a ese edificio en particular.

Para el del servidor VPN, se aconseja que tenga la misma funcionalidad sin importar el edificio, y que pueda identificar tanto a usuarios de Casa Matriz como de Sucursal, de forma tal que, en caso de no poder comunicarse con uno de los servidores VPN en una de las casas, se

pueda intentar acceder desde el otro. Deben tener su configuración espejada, aunque se debe reconocer que cada uno está en una red distinta, y actuar en consecuencia.

Se sugiere, además, la utilización de servicios de energía independiente, tales como UPS o conexión a grupo electrógeno, para los servicios más críticos del sistema (Routers, switches y servidores más importantes dependiendo de las incumbencias de la organización).

Es ideal que para todos los servidores existentes se encuentren copias de seguridad. Una forma económica de hacerlo es tener un servidor de backups general, que se actualice con cierta frecuencia, en donde se asegure la información que contienen todos los demás. Este servidor se puede encontrar en alguna de las sucursales, o si ambas se encuentran físicamente en zonas propensas a desastres naturales, puede ser en una locación a parte. Ciertamente esta opción no termina de asegurar la continuidad de un servidor caído, aunque permite tener una pronta recuperación de los datos ante cualquier eventualidad.

Si se quiere invertir un mayor presupuesto, lo cual es altamente recomendable, proponemos tener un servidor de backup para cada servidor de archivos y el de Mail, ya que son los más saturados de información, y se puede seguir manteniendo un único back-up para las configuraciones (DNS, VPN, Web, Users, DHCP, Intranet, Telefonía).

De la misma forma, dependiendo del presupuesto que se desee implementar, se pueden usar adicionalmente servidores espejados tanto como para back-ups, como para mantener la disponibilidad del servicio ante algún accidente en el principal. Ésta última configuración es ideal para todos los servidores, aunque, por razones de presupuesto, se pueden priorizar los más importantes para la organización.

Idealmente, por razones de disponibilidad de los servicios hacia el mundo exterior, se sugiere contratar ISPs que no posean problemas de corte de servicio (Servicio de internet de alta disponibilidad).

Además, sería correcto que el ISP provea de una conexión simétrica, de forma tal de asegurar comunicaciones rápidas, ya que la empresa muy factiblemente necesite de un gran ancho de banda para la conexión VPN y la actualización de los servidores de archivos, y generalmente, la velocidad de subida es mucho menor al necesario para compartir archivos.

Como alternativa para las copias de seguridad se puede utilizar servicios en la nube como ‘Google Drive’ o ‘Dropbox’. Estos servicios suelen solucionar el problema físico para el resguardo de información, pero pueden ser considerados peligrosos, ya que el dispositivo físico donde se guarda la información sensible de quien los contrata, pertenece a estas prestadoras.

Recomendaciones para maximizar la confidencialidad e integridad de la información.

Para empezar, se recomienda el uso de usuarios y grupos, para poder asegurar que nadie pueda acceder desde dentro de la organización a información correspondiente a áreas distintas de las necesarias. Esto permitiría que sólamente los de “Compras” puedan acceder a los archivos correspondientes a “Compras”, los de “Tecnología” al área de “Tecnología”, y así sucesivamente; de ésta manera se asegura el principio de Mínimo Privilegio. Así se puede tener un log del uso de los archivos y los usuarios y grupos, permitiendo ver quienes fueron responsables de los cambios a los archivos.

Además se puede agregar un IDS de Filesystem en todos los servidores, priorizando los de archivos, con el objetivo de ser notificado por algún uso indebido.

También es importante el uso de un IPS de host (como Fail2ban, por ejemplo) en todos los servicios que puedan ser accedidos desde dentro de la organización, priorizando los de archivos y usuarios, y donde se encuentre la liquidación de sueldos, con el fin de proteger el servidor de un ataque proveniente de la red de la organización.

Entendiendo la diferencia entre IDS (Sistema de Detección de Intrusiones) e IPS (Sistema de Prevención de Intrusiones), se aconseja el uso de alguno de los dos para la red de la organización, situados en los router de borde, y en los router de las DMZ de los servidores. Es ideal el IPS ya que previene además de informar.

Es de suma importancia que el sistema de liquidación de sueldos esté en un servidor diferente al servidor donde se aloja el sitio web de la organización, ya que éste último suele ser objetivo de ataques y, en caso de que falle la seguridad del mismo, se podría conseguir acceso no deseado a información sensible.

Considerando el servicio web que ofrece la organización, se aconseja el uso de un WAF (Firewall de Aplicación Web), de forma tal de proteger al servidor Web de posibles ataques tanto internos como externos. No obstante esto, es ideal una programación segura de la aplicación.

Sería correcto mantener toda la información cifrada, tanto en los servidores internos como externos, de forma tal que, sólo los usuarios y programas que deban poder acceder a ésta puedan descifrarla.

Se sugiere, la capacitación y concientización del personal sobre el uso de PGP. También la creación de un círculo de claves PGP para poder enviar correos electrónicos seguros y manteniendo el no-repudio. Este tipo de tecnología permite que la comunicación tanto interna como con los clientes pueda ser íntegra y confidencial.

Es también recomendable, para mantener la confidencialidad, que las comunicaciones del servidor web se hagan a través de HTTPS.

Acerca de compartición de archivos entre sucursales y con Clientes

Como describimos anteriormente, la compartición de archivos debe darse mediante el uso de Usuarios y Grupos, de manera tal que los usuarios de un área (pertenecientes a un grupo), sin importar la sucursal en la que se encuentren, tengan acceso a los archivos correspondientes a dicha área.

Respecto a los Clientes, se desconoce la forma actual en la cual comparten activos. Existen muchos medios, pero de nuestra parte aconsejamos el uso de mails cifrados y firmados, o el acceso a un servidor específico. Para el uso del servidor se les debe crear a los clientes usuarios y grupos, de esta forma se puede controlar la información y servicios que se les brinda, y el acceso sea únicamente a través de una red VPN dedicada.

Sobre servicios de almacenamiento de información en la nube

Si bien existen servicios de almacenamiento en la nube, solo se indica su uso para archivos personales de los miembros de la organización que no requieran back-up ni confidencialidad, dado que sobre éstos servicios no se puede asegurar la confidencialidad de los archivos almacenados en ella.

En caso de requerirse, la mejor forma de asegurar la confidencialidad, es a través de asesoramiento legal acerca de los términos y condiciones de uso del servicio.

Acerca del uso irrestricto a internet

Los beneficios de tener uso irrestricto de internet es tener un empleado que puede buscar metodologías y soluciones ya existentes, así como refrescar conocimiento para el trabajo que tiene que hacer. Al mismo tiempo, la empresa suele comunicar a los empleados, cierta información a través de diversas redes sociales, y este uso irrestricto facilita el acceso a esa información. Por otra parte, permite tener un empleado relajado, ya que puede en un pequeño descanso, usar el internet de forma recreativa, y limpiar su mente para seguir trabajando.

Las desventajas de ésto es que en el momento de recreación o simplemente de chequear alguna de las redes sociales de la organización, incluso buscando información sobre el área de trabajo, puede encontrarse con algún software malicioso o con alguna página web que robe sus credenciales de la empresa (con alguna de las técnicas de páginas vulnerables como CSRF o XSS) o comprometa la seguridad del host utilizado para ello. También aumenta las probabilidades de filtrado de información sensible de la empresa, por lo que se recomienda un contrato de confidencialidad. Por otra parte, es probable que la producción sea reducida en cierta medida por la ansiedad y el tiempo utilizado al chequear las redes sociales.

Se recomienda tomar una decisión sobre si mantenerlo o no, conociendo las ventajas y desventajas, y poniendo como prioridad la funcionalidad que requiere la organización.

En caso de querer mantener el uso irrestricto de internet, es aconsejable ampliar las medidas de firewall e IPSs o IDSs para disminuir los riesgos, así como también instalar software antivirus en todos los dispositivos con acceso a internet.

Una opción de control y registro, es tener un servidor entre el router de salida a internet y las redes de usuarios, donde se esté guardando la actividad de red que tienen los empleados con internet. Es una técnica invasiva, por lo cual, de implementarse, se deben renovar los contratos de los empleados con cláusulas que les informe sobre el uso de este mecanismo, y acepten que todo su tráfico de internet quede guardado y pueda ser analizado.

Acerca de los usuarios móviles

Para los usuarios móviles, se aconseja el uso irrestricto a internet, con la particularidad de que no pueden acceder a ningún servicio privado de la organización. De ésta manera si un usuario utiliza un dispositivo móvil vulnerable o malicioso, no podrá afectar al resto de los dispositivos.

Para ello se requiere, como antes fue mencionado, en las recomendaciones acerca de la topología, que la red de usuarios móviles se encuentre en una red privada, dedicada solo a ello, conectada directamente al router de borde, y que, mediante restricciones de Firewall, impida la comunicación con cualquier otro sector distinto a internet.

Acerca de medidas contra usuarios maliciosos

A lo largo del documento se van detallando distintas medidas, que, por más de estar encasilladas dentro de secciones diferentes a ésta, su objetivo principal es evitar el acceso de usuarios maliciosos a los diferentes activos de la organización (a través de Firewalls, IDS, IPS, WAF, redes dedicadas, políticas de acceso,etc.).

Se aconseja el uso de Firewalls de red, con políticas restrictivas en la mayoría de los dispositivos de capa de red, haciendo excepciones a todo tipo de conexión que se deba mantener. De esta forma asegurar que ningún host pueda comunicarse con otro que no debe (Marketing con Administración, por ejemplo), y solo permitiendo que las comunicaciones se den a través de teléfono o mail interno. Este tipo de configuración protege a los empleados y a los hosts internos de posibles usuarios maliciosos.

Para proteger todos los activos de la organización de un posible ataque por malware a través de un usuario interno, se recomienda bloquear los puertos usb y configurarlos únicamente al uso que van a tener, es decir, únicamente permitir teclado donde se va a conectar el teclado, únicamente permitir mouse donde se va a conectar mouse, y así con todos los dispositivos que sean de realmente necesarios. Esta configuración no es completamente imprescindible pero su implementación impide que los usuarios, intencionalmente o no, puedan utilizar algún dispositivo malicioso, o llevarse información.

Se debe considerar la idea de la creación de un CSIRT (Computer Security Incident Response Team) , con el objetivo de tener una rápida respuesta a los incidentes que puedan llegar a ocurrir. La implementación de esta idea le da prestigio a la organización, ya que asegura tener activos trabajando en la seguridad de la empresa.

Acerca de la evolución de la tecnología y el surgimiento de soluciones que cambian los paradigmas de la seguridad tal como se conocían hasta hace un par de años, tales como:

- ## Aplicaciones en la nube y SaaS (Software como Servicio)

Las aplicaciones en la nube son beneficiosas ya que reducen el costo de tener y mantener un servidor dedicado para algún tipo de programa de mucho peso. Este tipo de servicios, al estar en la nube, lo único que necesitan para su uso es un dispositivo con conexión a internet. Pueden tener modo mixto, esto significa, que se puede usar una aplicación local que actualice constantemente con la nube, y, si se pierde la conexión a internet, se pueda seguir utilizando y luego actualizar los datos cuando haya conexión.

Los problemas que este tipo de aplicaciones pueden generar son:

- Controlar quienes de la organización tienen acceso y de qué manera.
- En caso de dejar de pagar el monto mensual para su uso, se pierde el acceso a ellas, al igual que la información de una sola copia.
- No se tiene certeza de la confidencialidad de la información sensible que usa o almacena la aplicación.
- No se conoce la infraestructura de los servicios, y éstos podrían ser vulnerables.

Dicho esto, para el uso de este tipo de servicios, recomendamos de asesoramiento legal para asegurar la confidencialidad de la información, y al igual que si se utilizara una aplicación desde dentro de la organización, que se utilice un sistema de usuarios. Si la aplicación no lo tuviera, recomendamos utilizar una que si lo ofrezca. Así mismo, para asegurar la continuidad de un servicio, se puede contratar el tipo de aplicación mixta, ya que permite que se pueda trabajar momentáneamente sin conexión.

- ## Movilidad

La movilidad afecta a la seguridad de la información de manera que nos obliga a diseñar un sistema de seguridad aparte o específico para los dispositivos móviles, desde redes solo inalámbricas hasta conexiones VPN para usuarios remotos y las reglas de seguridad deben ser diferentes para cada caso.

- ## Internet de las cosas (IoT)

El internet de las cosas, si bien trae los beneficios de acceder o utilizar de manera remota o automática a nuestros dispositivos, también trae consigo una gran carga a la

parte de seguridad informática. Debemos estar muy atentos al configurar un dispositivo y su router, de manera tal que permita acceder a él y dar instrucciones sólo al personal autorizado.

- ## IaaS (Infraestructura como Servicio)

  Los servicios de infraestructura en la nube, traen problemas similares a los de almacenamiento o software en la nube, al ser, en general, software privativo, no se conoce las configuraciones de seguridad aplicadas sobre los mismos y no se puede modificar gran parte de ellas.

  Como conclusión, los riesgos principales relativos al uso del cloud.

  Los datos no están bajo el control directo de la empresa, ni en un contexto que responde a las lógicas empresariales, es decir que los datos están expuestos a las vulnerabilidades de terceros.

  La cesión y al uso de los datos. Esto es, los contratados pueden vender estadísticas sobre la información que manejan, o sea, usar estadísticas sobre la información de la empresa como activo para vender.

  La localización de los servidores del proveedor puede ser origen de conflictos con las normativas de protección de datos.

  El uso de las API, interfaces de tipo aplicativo que pueden ser usadas para construir otros servicios basándose en los existentes. Las API tienen que ser seguras puesto que son un punto de acceso a los datos.

  En general, el mayor problema de seguridad que tienen la mayoría de estas nuevas soluciones recae en la confidencialidad de la información y sobre el control de la seguridad.

  Como recomendación para contratar cualesquiera de ellos, es, conocer el historial del proveedor, si es posible el código fuente, y asesoramiento legal sobre el manejo y protección de datos que ofrezca el servicio al contratarlo.