María Isabel López Romero
Sistemas infromaticos. 1º DAW

PLAN DE SEGURIDAD DE UNA EMPRESA

INTRODUCCIÓN

Tenemos que hacer un análisis de la seguridad de la empresa en la que trabajamos y los posibles riesgos a los que nos enfrentamos para así proponer un plan de seguridad eficaz capaz de protegernos de las amenazas.

Nuestra empresa se dedica a la venta de productos, y lo hace tradicionalmente en tiendas físicas y también por tiendas online, tanto al por mayor como a la venta al publico general. La instalación informática de la empresa consta de una única red a la que se conectan los empleados de todos los departamentos para acceder a servicios como el correo electrónico, web, herramientas de gestión interna, etc. Y es esta misma red es la que también da servicio a las tiendas online.

Antes de entrar a analizar los riesgos que entraña esta estructura de red se define a continuación que es la seguridad informática y se justifica la necesidad de tener un plan de seguridad en nuestra empresa.

La seguridad informática puede definirse como un conjunto de medidas de prevención y detección de riesgos, amenazas, vulnerabilidades y cualquier otro tipo de eventualidad que pueda afectar un dispositivo o conjunto de ellos.

Un plan de seguridad informática es el documento donde se refleja el sistema de seguridad informativa de una organización (conjunto de medios administrativos, técnicos y personales que garantizan la seguridad informática.) Este plan debe recoger claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

MOTIVACIÓN PARA EL PLAN DE SEGURIDAD INFORMÁTICA.

En este apartado se explica los riesgos existentes que pueden comprometer la seguridad de la información y que justifica la necesidad de definir un plan de seguridad.

Amenazas físicas

Existen amenazas relacionadas con fallos humanos, con ataques malintencionados o con catástrofes naturales que afectan al sistema físico de nuestra instalación informática. Estas son daños físicos o robo del equipamiento y medios de almacenamiento de información. Por ejemplo, un incendio, una inundación, caídas de los aparatos, robos.

Amenazas lógicas

Las amenazas lógicas hacen referencias a aquellas que atacan nuestro sistema informático por medio de software. Un programa malicioso es cualquier tipo de software que realiza acciones

dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario, por ejemplo el robo de información, dañar o causar un mal funcionamiento el sistema informático, provocar un perjuicio económico, chantajear al propietario de los datos del sistema informático, permitir el acceso de usuarios no autorizados, provocar molestias o una combinación de varias de estas actividades.

Los distintos tipos de ataques a los que se enfrenta una organización son los siguientes:

Virus: secuencia de código malicioso que se aloja en fichero ejecutable (huésped) de manera que al ejecutar el programa también se ejecuta el virus. Tienen la propiedades de propagarse por reproducción dentro de la misma computadora.

Gusano: malware capaz de ejecutarse por sí mismo. Se propaga por la red explotando vulnerabilidades para infectar otros equipos.

Troyano: programa que bajo apariencia inofensiva y útil tiene otra funcionalidad oculta maliciosa. Típicamente esta funcionalidad suele permitir el control de forma remota del equipo (administración remota) o la instalación de puertas traseras que permitan conexiones no autorizadas al equipo. Los troyanos no se reproducen.

Bomba lógica: programas que se activan cuando se da una condición determinada causando daños en el sistema. Las condiciones de ejecución típicas suelen ser que un contador llegue a un valor concreto o que el sistema esté en una hora o fecha concreta.

Adware: muestran publicidad no solicitada de forma intrusiva provocando molestias.

Spyware: envía información del equipo a terceros sin que el usuario tenga conocimiento. La información puede ser de cualquier tipo como por ejemplo información industrial a datos personales, contraseñas, tarjetas de crédito, direcciones de de correo electronico (utilizable para enviarles correos basura) o información sobre páginas que se visitan (usable para seleccionar el tipo de publicidad que se le envía al usuario). Los autores de spyware que intentan actuar de manera legal pueden incluir unos términos de uso, en los que se explica de manera imprecisa el comportamiento del spyware, que los usuarios aceptan sin leer o sin entender.

Ransoware o criptovirus: software que afecta gravemente al funcionamiento del ordenador infectado (ejemplo cifra el disco duro o lo bloquea) infectado y le ofrece al usuario la posibilidad de comprar la clave que permita recuperarse de la información.

Keylogger: software que almacena las teclas pulsadas por el usuario con el fin de capturar información confidencial como contraseñas o número de tarjeta de crédito o conversaciones de chat.
Stealer: roban información privada guardada en el equipo. Típicamente al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas recordadas, por ejemplo en los navegadores web o en clientes de mensajería instantánea.
Rogueware: es un falso programa de seguridad que no es lo que dice ser, sino que es un malware. Por ejemplo falsos antivirus, antiespía, cortafuegos o similar.

Decoy o señuelo: software que imita la interfaz de otro programa para solicitar el usuario y contraseña y así poder obtener esa información.

Secuestrador de navegador: son programas que realizan cambios en la configuración del navegador web.

Wiper: es un malware orientado al borrado masivo de datos. Por ejemplo discos duros o bases de datos.

Criptominado malicioso, en inglés *Cryptojacking*: es un malware que se oculta en un ordenador y se ejecuta sin consentimiento utilizando los recursos de la máquina (CPU, memoria, ancho de banda,...) para la minería de criptomonedas y así obtener beneficios económicos. Este tipo de software se puede ejecutar directamente sobre el sistema operativo de la máquina o desde plataforma de ejecución como el navegador.

Web skimming: software que los atacantes instalan en aplicaciones webs de comercio electrónico con el fin de recopilar información de pago (datos personales y de tarjetas de crédito fundamentalmente) de los usuario que visiten dicho sitio web comprometido.

Amenazas persistentes avanzadas asociada, en los últimos años está apareciendo un malware, que son campañas fuertemente orquestadas realizadas por grupos asociados a estados o a importantes instancias con poder, cuyo objetivo más habitual es el robo de información estratégica o producir daños en sistemas de ciertas organizaciones.

Por ultimo cabe destacar el **malware como servicio,** que consiste en organizaciones de ciberdelincuentes que ofrecen servicios de programas maliciosos ilegales en la nube (por ejemplo para interrumpir operación, robar datos, etc). Estos servicios son accesibles desde cualquier lugar y son extremadamente fáciles de usar. Cualquiera los puede usar y por tanto se les pueda vender a cualquiera.

INSTALACIONES E IDENTIFICACIÓN DE RIESGOS.

Una vez conocemos los posibles riesgos a los que nos enfrentamos se procede a hacer un análisis de la vulnerabilidad de nuestras instalaciones.

Por un lado, cabe destacar que nuestra empresa es una PYME, y esta expuesta a ciberataques igual que el resto de empresas, pero tiene la vulnerabilidad añadida que al ser una PYME, se suele invertir menos recursos en redes de seguridad, esta menos informados de los cambios tecnológicos constantes y las diversas amenazas a la que se exponen día a día, ademas a esto suma que tienen una capacidad limitada para invertir en recurso y a que hay poca cultura sobre seguridad de la información, y un menor controlo sobre las conexiones a Internet.

Publicar este servicios (web para compras) en Internet desde la red a la empresa aumenta el riesgo de sufrir un incidente de seguridad. La empresa cuenta con una única red a la que se conectan tanto los empleados como los clientes para realizar compras y esto es una vulnerabilidad evidente ya que si alguien consigue acceder a un dispositivos de esta red, podrá acceder a todos y hacerse con el control de la información.

A continuación se propone una instalación informática que suple esta vulnerabilidad:

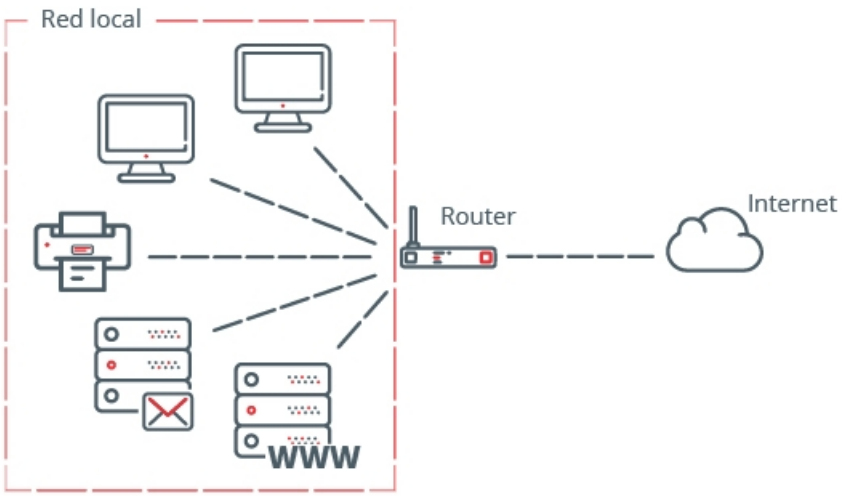
1. Firewall y DMZ

Como ya hemos dicho esta empresa tiene una única red interna local, a la cual se accede a distintos servicios desde Internet, por un lado los empelados acceden a su correo y a las herramientas de gestión que utilicen , y a su vez clientes acceden a su pagina web para efectuar compras.

Esta empresa tiene servidores propios y gestionan su propia información, lo que supone por un la que es la organización la que tiene que afrontar la seguridad de la información, esto es una ventaja porque ellos son en todo momento quien controlan la información y no la gestiona un tercero, pero a la vez es un reto, al tener que afrontarlo con sus propios recursos.

El principal problema que se presenta es que tanto los empleados como los clientes se conectan a la misma red, lo que aumenta el riesgo de sufrir un ataque, en cuando un ciberdelincuente logre acceder a uno de los dispositivos conectados a esta red, podrá acceder a cualquiera.

En esta imagen se muestra de manera grafica como esta funcionando actualmente la organización.



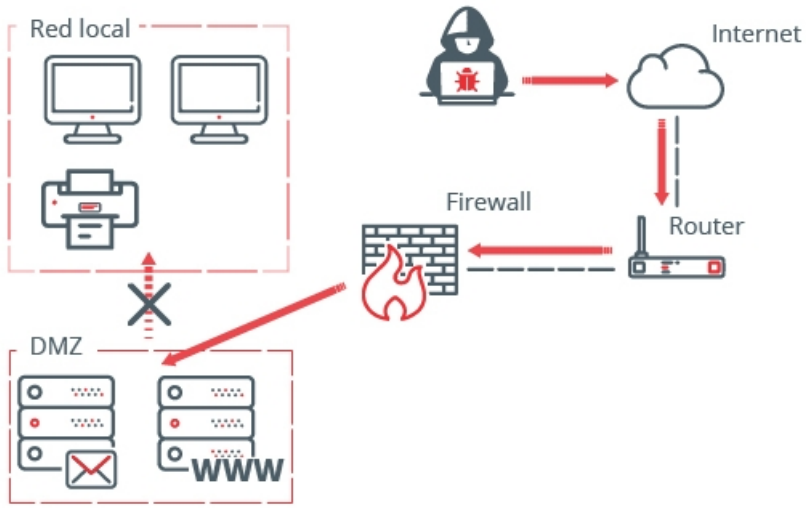
Para evitar los riesgos derivados de que se acceda al servidor desde Internet se debe utilizar un cortafuegos o firewall y una red local denominada zona desmilitarizada o DMZ.

El cortafuegos es un dispositivo de seguridad cuya función principal es la de filtrar el tráfico de red entrante y saliente por medio de una reglas, que permitirán su paso o lo rechazarán. De esta forma cuando se intente acceder al servidor, el cortafuegos evaluara la petición, y se aceptara o rechazará.

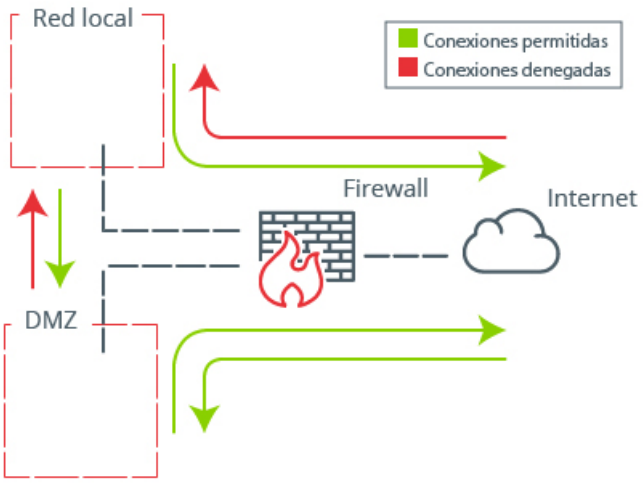
Es conveniente que el cortafuegos sera dedicado, porque cuenta con más capacidades de procesamiento que los basados en software, ya que se diseñada específicamente para esa tarea.

Por otra parte una zona desmilitarizada es una red aislada que se encuentra dentro de la red interna de la organización. Pero en ella se encuentran ubicados solamente los recursos que son accesibles desde Internet, como el servidor web o de correo.

La DMZ permitirá las conexiones procedentes tanto de Internet, como de la red local de la empresa, pero las conexiones que van desde la DMZ a la red local, no están permitidas. Esto es porque los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad y de esta forma, al estar denegado el acceso desde el DMZ a la red local, sera mas difícil acceder a ella.

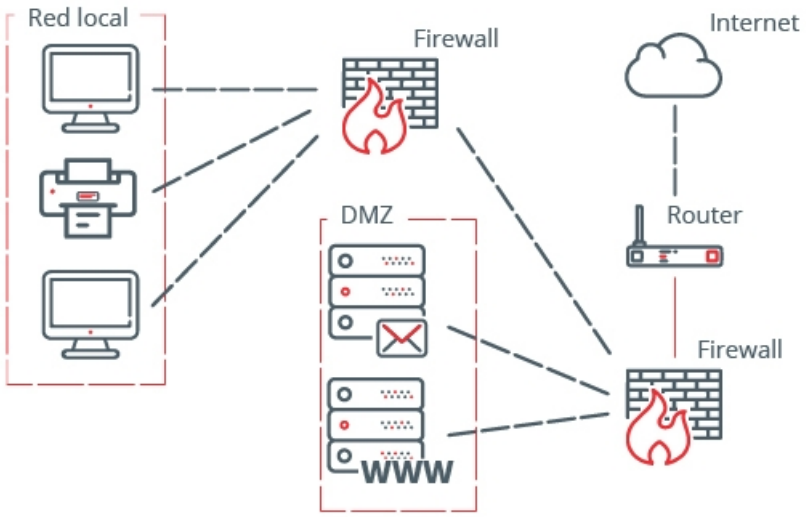


El firewall. será el encargado de segmentar la red y permitir o denegar las conexiones.



Como se ve en la imagen, si se efectuá un ataque no podrán acceder a la red local, donde este la información, ya que no se puede directamente por el firewall, ni a través del DMZ. Podrán acceder a esta zona ya que tiene acceso a Internet porque ahí esta la pagina web para comprar los productos, pero desde ahí no pueden acceder a la red local.

Si queremos aun mas aumentar la seguridad de nuestra red interna frente a un ataque proveniente de la DMZ, se propone ubicar dos firewall.



Por ultimo , se propone también utilizar otras herramientas de motorización, detección y prevención, para proteger la DMZ, como son los IDS e IPS, y también es recomendable mantener actualizados a la última versión disponible todo lo que tengamos en la DMZ.

A parte de aislar el servicio de la red local de la empresa, es conveniente incorporar también las siguientes buenas practicas para mejorar su seguridad:

2. Conciencia los trabajadores

Es imprescindible sensibilizar a los trabajadores de la empresa sobre los efectos negativos de la pérdida de información, así como sobre el impacto que tiene que una amenaza entre en el sistema.

La gran mayoría de los virus y malwares que ingresan a redes corporativas se debe al mal uso de Internet por parte de los colaboradores, que muchas veces ingresan a sitios web no seguros o abren e-mails maliciosos provocando que se permita la entrada de programas maliciosos como el ransomware; el cual le permite al hacker secuestrar todo el sistema y pedir un rescate por la información.

Por ello, y como parte de una política de seguridad, en la red de cualquier empresa conviene aplicar el principio del mínimo privilegio, permitiendo el acceso a la información solo a aquellos trabajadores que la necesiten estrictamente y estableciendo quién puede acceder a cada tipo de información. Una adecuada capacitación de todo el personal de la pyme en el ámbito de la seguridad informática nunca está de más, y, de hecho, permitirá que cualquier evento de riesgo pueda ser atendido de la mejor manera posible.

3. Usar un servicio de firewall profesional

A todo lo que ya hemos explicado del firewall conviene añadir que si bien existe una infinidad de servicios gratuitos en la red, estas versiones suelen ofrecer un servicio con funcionalidades limitadas y con una protección muy básica ante ataques informáticos, por lo que lo más conveniente es contratar un servicio que se encargue de toda la gestión de la red de seguridad de su empresa y que pueda brindar una asesoría técnica continua.

4. Software antimalware

Un software antimalware es un programa diseñado para prevenir, detectar y solucionar los problemas causados por archivos maliciosos que entran en contacto con los dispositivos personales o redes. Por ello, un software de seguridad robusto es la piedra angular sobre la cual se basa cualquier plan de seguridad.

Es importante contar con una licencia que pueda cubrir todos los equipos informáticos de la empresa.

5. Configurar filtros contra SPAM en el e-mail corporativo

El correo electrónico es una de la vías de comunicación mas utilizadas, por ello es utilizada por los ciberdelincuentes para perpetrar ataques, a través de e-mails masivos que contienen adjuntos maliciosos o enlaces a sitios inseguros. Estas malas prácticas pueden generar diversos problemas en la red corporativa e, incluso, contener ransomware.

Es imprescindible contar con medidas de seguridad en los servidores y soluciones antispam a través de diversos servicios ofrecidos en el mercado. Paralelamente, será importante explicar a los trabajadores la importancia de un buen uso del correo electrónico corporativo y de no manejar información sensible en cuentas de correo personales.

6. Actualizaciones de software y utilizar uno legal.

Las actualizaciones de software hacen entre otras muchas mas cosas, reparar vulnerabilidades detectadas en un sistema operativo o un programa de software.

Utilizar un software legal significa poder contar con soporte técnico y de actualizaciones del fabricante.

7. Realizar copias de seguridad fiables.

Es importante también tener un adecuado plan de recuperación ante ataques que pudieran comprometer archivos con información importante. Por ello, se hace necesario contar con un buen backup. para reducir así los tiempos de recuperación y minimizando los daños.

8. Contar con un equipo especializado en seguridad informática

Aunque esta vez han sido los empleados los encargados de diseñar el plan de seguridad, seria conveniente que contara con un personal especializado en el área. Esto facilitará que las estrategias y planes de seguridad informática puedan aplicarse del modo correcto, y con el menor riesgo posible de errores humanos, determinará protocolos de actuación en caso de ataque. Si la empresa es muy pequeña, este servicio puede externalizarse.

10. Uso de contraseñas seguras

Usar contraseñas seguras en todos los dispositivos y aplicaciones que se encuentren en la empresa es muy necesario como medida preventiva.

11. Capacitacion de todo el personal

Una adecuada capacitación de todo el personal de la empresa en el ámbito de la seguridad informática permitirá que cualquier evento de riesgo pueda ser atendido de la mejor manera posible.

Por ultimo, algunas medidas dirigidas a la seguridad en cuanto a amenazas físicas son, sistemas anti incendios y anti inundaciones, sistemas de refrigeración, sistemas de alimentación ininterrumpida (S.A.I), cámaras de seguridad, accesos restringidos a los recintos.

CONCLUSIÓN

Como conclusión esta empresa tiene vulnerabilidades al no contar con un plan de seguridad firme ni con un equipo especializado en seguridad. Tras analizar las redes de la empresa, se detecta que existe un riesgo evidente al solamente contar con una única red a la que se conectan todos los dispositivos de la empresa, a la vez que también es la misma que se utiliza para la tienda online, pudiendo de esta manera acceder de manera muy fácil a la red local de la empresa. Para solventar este problema se propone crear una Zona Desmilitarizada para aislar a la red local y protegiendo de esta manera la información, ademas, añadiendo cortafuegos reducimos considerablemente el riesgo de ser atacados. Junto con esto se suman otras medidas de seguridad como conciencias y cap atizar a los trabajadores, tener software dirigidos a la seguridad, que sean legales y tenerlos actualizados constantemente, controlar el correo electrónico y el uso de contraseñas seguras, entre otras.

BIBLIOGRAFÍA

https://uss.com.ar/corporativo/medidas-de-seguridad-informatica-pyme/

https://www.acronis.com/es-es/solutions/business/mid-size-business/
https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/tipos-de-seguridad-informatica/

https://destinonegocio.com/pe/gestion-pe/6-tips-para-fortalecer-la-seguridad-de-la-informacion-en-su-pyme/

https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa