01 de noviembre de 2022

Propuesta de Mejora de Ciberseguridad

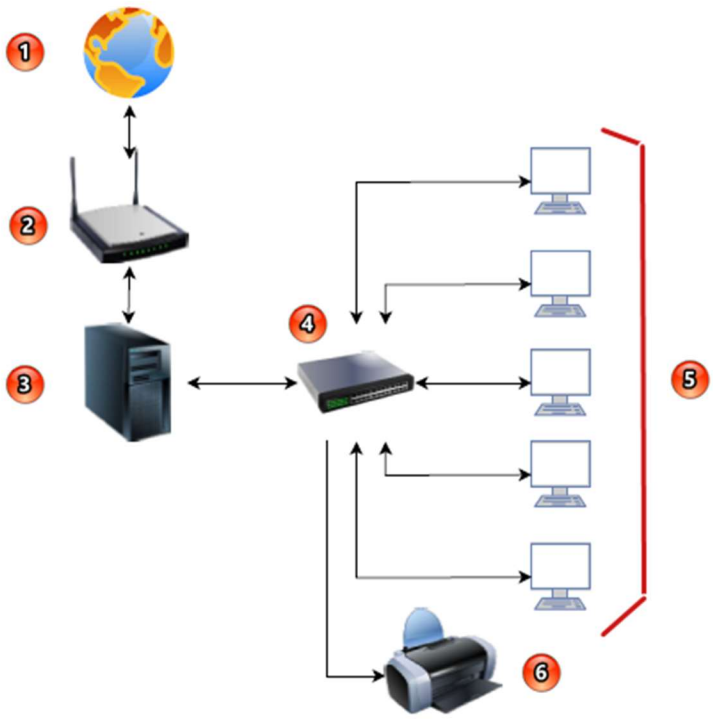
El día 27 de abril de 2022, la empresa LexCorp sufrió un ataque de un malware, el cual afectó a la totalidad de los equipos, cifrando todos los datos que contenían estos.

A raíz de ese incidente, nos solicitan un informe sobre el ataque para determinar origen y daños causados y posterior a esto, una propuesta de mejora para evitar sufrir nuevamente este tipo de ataques.

Lo primero que se realiza es una investigación de la estructura de red y los usuarios finales y eventuales:

Esquema de red:

Diagrama de Red Actual



Referencias:

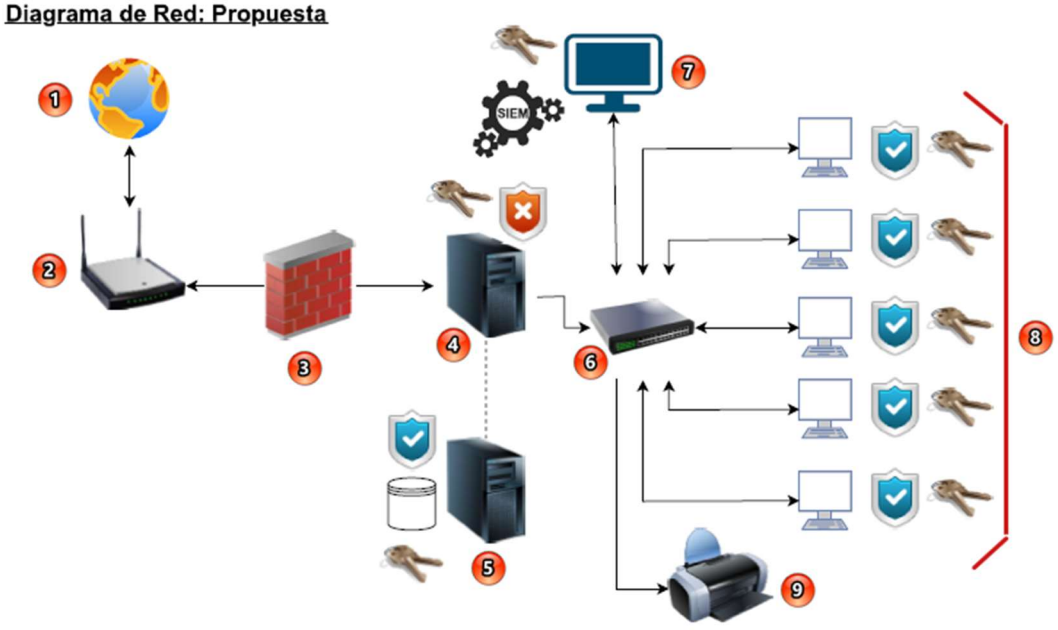
1) Internet
2) Router (ethernet + wifi)
3) Servidor
4) Switch
5) Terminales
6) Impresora

Posterior a esto, se indaga sobre la red y accesos a la misma. Determinando que la red es simple, sin restricciones y con muchas vulnerabilidades teniendo en cuenta que los usuarios finales y permanentes son cinco (5), mientras que los usuarios eventuales son tres (3), y en donde todos los mencionados, aparte de conectarse a la red en sus terminales, también lo hacen con sus dispositivos móviles o notebook personales.

En conclusión, las vulnerabilidades son altas y requieren una acción inmediata en el corto plazo.

A continuación, se expone la propuesta de mejoras en forma gráfica:

Diagrama de Red: Propuesta



Referencias:

1- Internet
2- Router (ethernet + wifi)
3- Firewall
4- Servidor Principal
5- Servidor Backup
6- Switch
7- SIEM – IDS/IPS
8- Terminales
9- Impresora

Detalle de propuesta para control de Perímetro:

Como primera medida, se recomienda implementar una barrera firewall (2) desde la conexión a internet externas a la red interna de la empresa. Seguido de esto, la configuración para el servidor (4) que se debería implementar es la siguiente:

- Antivirus con licencia en el servidor y en todas las terminales.
- Administración de credenciales de usuarios aplicando políticas de grupo para acceder a determinados directorios y aplicaciones.
- Servicio de RDP para las conexiones permitidas en el controlador de dominio.
- Limitar y administrar el tiempo de conexión/desconexión de usuarios internos y externos.
- Bloquear la instalación de programas en todas las terminales.
- Limitar el acceso a internet generando un repositorio de webs visitadas con frecuencia para configurar como excepciones para determinados usuarios.
- Monitoreo de archivos adjuntos recibidos, permitiendo la descarga previo análisis de agente.
- Bloqueo de puertos USB de todas las terminales.
- Bloqueo y/o retiro de lectoras de CD (si las hubiere).
- Administración y monitoreo de dispositivos externos que pueden conectarse a la red, ya sea de manera física (ethernet) o por wifi. Configurar una red invitados para este tipo de casos.

Por otro lado, se recomienda configurar un equipo (7) exclusivamente para el monitoreo del tráfico de datos e interacciones en la red mediante un software del tipo SIEM (Seguridad de la información y gestión de Eventos). El mencionado equipo por medio del switch estará interconectado con todos los equipos de la red. Como complemento, se sugiere implementar tecnología de IDS/IPS para detectar ingresos no autorizados como así también el tráfico de datos de manera sospechosa.

Otra media para tener en cuenta es la implementación de un servidor de backup (5), el cual NO va a estar conectado de manera directa a la red, sino que, de acuerdo a una frecuencia a definir, se conectará y se correrá una rutina de copiado de la información total del servidor siempre y cuando no existan alarmas o eventos captados por el SIEM. Otra opción a contemplar es la contratación de un servicio de backup en la nube.

Para el resto de los equipos (8) aparte del antivirus local, se requiere una configuración de doble factor de autentificación al servicio RDP del servidor. Y como complemento muy importante, se requiere una capacitación para todos los usuarios finales en el uso responsable y seguro de las computadoras y la información de la empresa (confidencialidad).

Todas las propuestas mencionadas son escalables, por ende, se pueden planificar a corto/mediano plazo en este orden de prioridades:

Corto Plazo:

1) Capacitación de ciberseguridad y buenas prácticas para todo el personal.
2) Configurar un firewall para protección de las entradas y salidas de internet.
3) Antivirus en todas las terminales y servidor.
4) Configurar un Controlador de Dominio con reglas de acceso y permisos adaptables al negocio.
5) Bloqueo de puertos USB.
6) Configuración de red invitados y restricción de conexión de dispositivos externos.

Mediano Plazo:

1) Implementación de un equipo con SIEM, IPS/IDS.
2) Servidor de Backup.

Analista de Ciberseguridad: Elvis Galvalisi