Práctica de diseño de plan de seguridad
Grupo 10 - Escenario 2

Empresa ya consolidada que se dedica a brindar servicios informáticos. La mayoría de sus empleados trabajan de forma remota, pero hay algunos que lo hacen on site. Necesitan una intranet más segura. La información confidencial de la empresa tiene buena seguridad lógica, pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica. No tienen problemas en invertir dinero, pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.

1. Un análisis de la situación actual de cada empresa que se les haya asignado.
2. Para cada escenario planteado, crear un plan de seguridad.
3. Este plan debe ser de 6 pasos e incluir: seguridad lógica, física, pasiva, activa y controles de medida de seguridad y de vulnerabilidades que podrían explotar los atacantes.

Análisis de la situación actual

La empresa <Nombre de empresa> tiene como punto a favor el correcto uso de la seguridad lógica, aunque podrían mejorar por el lado de la seguridad física.

El hecho de que haya empleados remotos significa que deben hacer hincapié en los controles de acceso a los sistemas (VPN, intranet), equipamiento de seguridad física (por ejemplo vía autenticación de 2 factores).

Nos ha llegado también el informe que algunos empleados se resisten a nuevos cambios, por lo que creemos que las modificaciones deben ser de facto, a fin de no brindar ningún otro tipo de solución más que adaptarse a los nuevos protocolos de seguridad de la empresa, siempre convalidando con el plan propuesto y teniendo en cuenta que la seguridad es lo más importante a resguardar.

Es importante realizar también un relevamiento del servidor web a través del cual se contactan los clientes, no solo para verificar que la información (sensitiva) se guarde de manera segura si no para comprobar que sea redundante a fin de no perder ningún dato de cliente.

Plan de seguridad

1. **Seguridad lógica**: Para garantizar la seguridad de datos y sistemas, se recomienda incorporar un control de acceso, para ello, cada vez que inician sesión se le pedirá un usuario brindado por la empresa y una contraseña creada por el usuario, la misma deberá ser personal y confidencial. Además se instalará en cada computadora un antivirus para ayudar a detectar, evitar y eliminar posibles malware, este se ejecutará automáticamente para brindar protección en tiempo real. Se incorporará un firewalls para bloquear el acceso no autorizado.

2. **Seguridad física:** Se recomienda el uso **obligatorio** de dispositivos físicos token (RSA) o como mínimo de software (google authenticator) para loguearse a toda aplicación como VPN, email o cualquier otro sistema que contenga información sensitiva o de acceso a cualquier red interna de la empresa. Se recomiendan también el respaldo de datos (backups) de todos los equipos que contengan información imprescindible asi como del servidor web, que también debe tener un sistema redundante.

3. Seguridad pasiva: Como primer medida en este punto sería necesario hacer copias de seguridad de la información más importante para la empresa, a través de particiones de disco como una herramienta accesible. También se debería llevar a cabo una periódica comprobación del funcionamiento del antivirus, para mantener sus sistemas libres de malware, esto por supuesto en conjunto con un escaneo y limpieza constante de los equipos de la organización.

4. Seguridad activa: Para identificar y prevenir los ataques en tiempo real, se recomienda el uso y empleo adecuado de las contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación de letras, números, mayúsculas, entre otros. Intentar no utilizar datos que puedan ser de conocimiento público (dirección, cumpleaños, etc.)
   Se recomienda también el uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
   Por último, encriptar los datos importantes (cifrar los datos o la información para que sólo pueda ser leído si se conoce la clave de cifrado)

5. Controles de medida de seguridad: Teniendo en cuenta que los empleados se resisten a nuevas medidas, es necesario implementar medidas directivas, disuasivas y preventivas para generar conciencia en los mismos de los nuevos riesgos que afrontan día a día y de los cuidados que deben tener. Fijar policies, políticas que deben ser comunicadas constantemente y carteles de advertencia previos a los envíos de emails, visitas a páginas que pueden resultar peligrosos, etc. son necesarios para mantener la seguridad de la empresa.

6. Controles de vulnerabilidades que podrían explotar los atacantes: debido al portal web por el que los clientes realizan los pedidos, el cual asumimos que accede a alguna base de datos de la empresa, es necesario implementar medidas (detectivas)

que busquen evitar potenciales ataques, siendo vitales la implementación de antivirus de calidad y firewalls; y en caso de sufrir algún ataque, o correr el riesgo de sufrirlo, la activación de medidas (correctivas) de seguridad que pueden llegar hasta la desconexión de los equipos, tanto los localizados físicamente en la empresa como los que acceden en forma remota, de la red.