Plan de seguridad.

Escenario:

- Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan on site y están dispuestos a recibir capacitación. Poseen actualmente dos personas encargadas de sistemas, las cuales manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa). No realizan copias de información porque no las creen convenientes. Poseen una página web donde hay catálogos y los clientes pueden hacer compras a través de la misma.

1. Análisis:

   En la empresa no se encuentra establecido un protocolo de seguridad por lo cual la información de sensibilidad debería estar visible para las personas del área encargada, por seguridad se deben realizar algunas copias de seguridad de la información para mantener la integridad de los datos.

   Teniendo en cuenta que la seguridad informática de la empresa no es la mejor, se diagnostica que el nivel de criticidad en cuanto a la captación de algún malware para obtener datos es realmente alta.

2. Plan seguridad:

   2.1. Seguridad Lógica:

   Implementar software que impidan que malware o Hacker’s puedan ingresar a las computadoras de la empresa y adicionalmente implementar protocolos de control de acceso, cifrado de datos, instalación de antivirus y recomendamos que según la capacidad financiera de la empresa incremente implementen un firewall para tener mayor control de la información.

   2.2. Seguridad Física:

   Se recomienda tener una puesta a tierra en la tomas de corriente para que los equipos no sufran alteraciones o también implementar una UPS para pérdida de energía que afecte los equipos puedan estar siempre activos. Se recomienda realizar un back-up de la página Web en caso de sufrir algún ataque informático directo a la web de ellos o respaldos semanales de la información sensible manejada por las personas encargadas de sistemas.

2.3. Seguridad Pasiva:

- Las medidas recomendadas en el 2.2. de back-up se realicen en diferentes dispositivos con diferentes ubicaciones
- Ejecutar el antivirus con una periodicidad diaria para detectar malware en el equipo.
- Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
- Cuando haya una infección por un virus, comprobar que el antivirus funcione correctamente.

2.4. Seguridad Activa:

- Se recomienda clave en la Web para los usuarios sea esta de mayor seguridad Alfanumérica con caracteres especiales.
- Se recomienda a los empleados manejar claves con una mayor seguridad para evitar la fuga de información.
- Encriptar los datos sensibles de los usuarios que realizan compras por medio de la web.

2.5. Controles de Medida de seguridad:

- Creación de política de seguridad informática y su divulgación a todos los empleados.
- Capacitar a los empleados en los diferentes ataques y más comunes malware evidenciados.
- Restricciones de instalaciones de programas no corporativos.
- Reportar correos sospechosos o mensajes maliciosos que puedan registrar los dispositivos de los empleados.
- Desconectar equipo de la red empresarial cuando se percatan de algún error no común o mensaje inesperado.

2.6. Vulnerabilidades:

- Remitir correos masivos para detectar la cantidad de empleados que pueden incurrir en la apertura de mensajes maliciosos y brindar capacitación directa a estas personas.
- Verificar la capacidad de respuesta del servidor de la página web ante ataques o algún bot malicioso que deje inoperativa la web.