Análisis de caso

Desafío – Riesgos de seguridad en entornos corporativos

José Miguel Rivera

Empresa “FastBuy”

Incidentes:

1. Incremento inusual en el tráfico del servidor web, provocando lentitud y caídas intermitentes del servicio.
2. Correos electrónicos sospechosos enviados a empleados con enlaces fraudulentos solicitando credenciales.
3. Registros en el firewall que muestran intentos repetidos de acceso no autorizado a la base de datos.
4. Inyecciones de código detectadas en los formularios de inicio de sesión de la plataforma

Requerimientos:

1. Explicar la importancia de la seguridad de la red en la empresa de comercio electrónico FastBuy. Además de describir como la confidencialidad, integridad y disponibilidad se ven afectados (2 Puntos)

Considerando que la empresa FastBuy es de tipo comercial y almacena en sus servidores una gran cantidad de datos personales y bancarios, cualquier tipo de incidente que genere una fuga de información, daño a los clientes o exposición de datos complicará la evolución y crecimiento de la empresa, debido a que los clientes perderán la confianza y los dueños entenderán que se exponen a sanciones legales y pérdidas económicas.

Confidencialidad: Esta se ve afectada debido a los ataques de phishing que están siendo recibidos en la red interna y es probable que ya hayan caído en el algunos empleados.

Integridad: Las inyecciones de código que se están recibiendo, que aparentemente pueden ser del tipo SQL inyection o a través de algún script programado busca vulnerar accesos de clientes y obtener su información incluso cambiarla.

Disponibilidad: Los ataques de DDoS que están generando un tráfico inusual terminarán por provocar una caída general del servidor.

2. Identificar y describir los activos más críticos para la empresa FastBuy (servidores, bases de datos, dispositivos de red). Clasificar los activos en función de su criticidad y justificar la clasificación realizada. (2 Puntos)

Activos críticos:

Se realiza la siguiente clasificación de activos considerando la infraestructura de red con la que cuenta FastBuy.

1. Servidores: Servidor de correo electrónico, servidor web, base de datos de clientes
2. Dispositivos de red: Routers y swtiches de red interna
3. Datos sensibles: Datos de usuarios
4. Aplicaciones: sitio e-commerce

3. Analizar los tipis de ataques que se están produciendo en Fastbuy y clasificarlos. También explicar el método que podrían haber utilizado los atacantes para llevar a cabo los ataques. (2 Puntos)

De acuerdo al análisis realizado los ataques recibidos serían los siguientes:

Ataques de denegación de servicio DdoS : Estos ataques se estarían realizando por medio de un bot que genera multiples conexiones al servidor provocando caídas y lentitud.

Ataques de inyección de datos SQL injection : Estos ataques se están realizando para revelar login y password de clientes para modificar su información y provocar pérdidas económicas en toda la empresa.

Ataques de suplantación y robo de informacón Phishing : Estos ataques van dirigidos al personal interno de la empresa para obtener información de los clientes y sus datos bancarios.

4. Identificar los riesgos específicos que estos ataques representan para Fastbuy. Además de evaluar el impacto potencia y la probabilidad de cada amenaza, asignándole una clasificación de bajo, medio o alto según es necesario. (2 Puntos)

Tipo de ataque	Análisis de impacto	Probabilidad	Clasificación
1.- Ataque de DDoS	Interrupción de servicio Caída de sistemas Desconfianza de clientes	Alta, los servidores no están respondiendo a la cantidad de conexiones y están saturándose lo que se ha observado en lentitud y caídas.	Alta, es de suma urgencia
2.- Phishing	Accesos no autorizados, credenciales, claves de servicios y servidores	Media, el personal interno debe estar consciente y capacitado en que estos direccionamientos a link falsos ocasionan robo de información.	Alta, se debe instruir al personal en estas materias.
3.- SQL Injection	Robo de información de clientes, ventas, información comercial, bancaria, crediticia, etc.	Alta, estos ataques comprometen la estabilidad del sistema, los datos de los clientes y su información privada.	Alta, Se ha observado que el firewall en sus logs registra múltiples intentos de accesos inválidos.

5. Proponer 2 estrategias para mejorar la resiliencia y disponibilidad en la red Fastbuy ante futuros ataques. (2 Puntos)

Se proponen las siguientes estrategias para mejorar en FastBuy

- Disponer de un servidor de respaldo y copias de seguridad de bases de datos e información critica.
- Capacitar, difundir e informar al personal interno los ataques que están llevándose a cabo en la empresa a fin de que se eviten las fugas de información por mal uso de correos electrónicos.
- Se sugiere instalación de servicios de monitoreo de servidores y visualización en pantallas tipo televisores que se generen alarmas cuando existan conductas inusuales.
- Mejorar servicios de correo electrónico que se vea aumentada la protección ante spam, phishing, ejecución de archivos adjuntos, etc.