Sesion 4-Cibersegurdiad en el sector comercio electrónico

Hecho por Santiago Noriega TELENTO TECH

Actividades para desarrollar

1. Identificación de Activos Críticos

Objetivo: Reconocer los elementos más valiosos que deben ser protegidos para garantizar la operación segura del negocio.

Argumento: En una empresa de comercio electrónico, los activos críticos son aquellos que sustentan tanto las operaciones como la confianza de los clientes. La pérdida o compromiso de estos activos puede causar interrupciones, pérdidas económicas, daños a la reputación o incluso sanciones legales.

Activos Críticos	ocupación	Nivel de Prioridad
BASE DE DATOS DE CLIENTES	Es un sistema de que almacena información y datos personales de los clientes.	ALTA
SERVICIOS WEB	Un servidor web es un ordenador que almacena, procesa y entrega archivos de sitios web. Consta de una parte de hardware y otra de software, y cada una de ellas desempeña un papel distinto en el procesamiento de archivos.	ALTA
CONTROLES DE PAGO	Los controles de pago en internet son procesos y mecanismos que aseguran la seguridad, precisión y autorización de las transacciones financieras realizadas a través de internet.	MUY ALTA

COPIAS DE SEGURIDAD O BAKUPS	Es un sistema que se encarga de hacer copias de tu información para recuperarla en caso de emergencia por hackeo o perdida de datos esto se hace muy a menudo en nuestros dispositivos con el fin de que nuestra información pueda recuperarse de manera inmediata en cualquier escenario posible.	MEDIA
CORREOS ELECTRONICOS CORPORATIVOS	Son correos electrónicos de empleados de una empresa cuya función es la comunicación con otros empleados del trabajo y junto en el tema de soporte técnico.	MEDIA
SEGURIDAD Y MONITOREO	Es una parte fundamental de una empresa que protege en todo momento cualquier de cualquier novedad que se le presente al sistema de una empresa con el fin de tomar acciones inmediatas para contrarrestar los problemas que se le acerquen al sistema por eso hay personas encargadas que monitorean todo esto desde el trafico de la red hasta los que entra y sale de los servidores centrales.	MUY ALTO

✅ 2. Análisis de Amenazas y Riesgos

Objetivo: Determinar los riesgos a los que están expuestos los activos críticos, evaluando el impacto y la probabilidad de cada amenaza.

Argumento: La evaluación de amenazas permite priorizar esfuerzos en la protección de activos y preparar respuestas eficaces. En el comercio electrónico, las amenazas más comunes incluyen el robo de datos, ataques de denegación de servicio, y malware.

El problema puede persistir de varias maneras ya que todo lo hace el atacante a que objetivo quiere llegar con la victima pero en este caso yo daré una manera mas optima que daños y amenazas podrían ocurrir si entramos en manos equivocadas.

BASE DE DATOS

NIVEL DE AMENAZA: PHISHING/RANSOMWARE/DDoS

IMPACTO: MUY ALTO Y PELIGROSO

PROBABILIDADES: VARIADAS

RIESGO: MUY CRITICO

¿Porque podría ocurrir esto?

El atacante podría enviar correo falso a sus victimas en un corto debido tiempo aparentando que es de un empleado de una empresa o de una un proveedor ya que si la victima ve que el mensaje tiene un link que no es seguro es una trampa llevan a su atacante a paginas falsas para robar credenciales e información si la victima es mas avispada no lo hará y si no sabe de la tecnología mejor dicho dio de papaya sus datos a un atacante después que pasa?. El atacante hace lo siguiente si ingreso sus datos como contraseñas y usuarios o algo mas que demuestre el atacante usa herramientas para descifrar y de ahí se cuela a la **BASE DE DATOS CENTRAL** entrando a la red desde un portal web ya que ellos pueden conectarse mediante acceso remoto usando VPN o encriptando su red para que sea inrrasteable

CONSECUENCIAS!

1.Extrae datos del servidor central puede ser archivos confidenciales o datos de otros empleaos para tener el poder

2.Modificar y eliminar cualquier clase de registro que el deje

3.Crear puertas traseras una táctica en la cual no podría dejar ninguna huella para que nadie sepa que el estuvo dentro de la red

4.lo que si podría ser mas peligroso y podría exponer y perder el acceso total y tener que pagar un rescate es un **RANSOMWARE.**

El infectara los servidores mediante sus técnicas como phishing o usando software después se empieza a propagar como un virus sin control afectando toda la red causando un error 404 si los archivos están cifrados con cualquier línea de seguridad obtiene todo el control del servidor y hace sus ataques.

¿COMO PODRIAMOS DETENER EL ATAQUE?

1.Se podría mejorar el tema de la seguridad con la red evitando que no quede expuesta para el atacante.

2.Tener herramientas que puedan mejorar aun mas la seguridad más allá

3.Tener respaldos de copia seguridad y un monitoreo constante de lo que entra y sale del servidor.

4.Estar al día con las actualizaciones y cambios del software de la base de datos.

SERVIDOR WEB (DDoS)

NIVEL DE LA AMENAZA: ALTA

AMENAZAS QUE PODRIAN AFECTAR: DDoS o Ransomware

PROBABILIDADES: DESCONOCIDAS

RIESGO: ALTO/CRITICO

El problema puede ocurrir de varias maneras pero algo descnocida porque no se sabe cunado y es que el atacante usa una técnica llamada BOTNET que es un troyano que convierte tu equipo en un arma para atacar a un servidor o a una victima y esto sucede ya que es un virus que se esconde muy fácilmente en cualquier aplicación insignificante ya que pocas veces un antivirus lo puede detectar pero que es algo que actúa como una especie de

zombie. El atacante usa esta técnica en cualquier parte del mundo para empezar atacar el problema de esto es que no hay control y a la vez es difícil rastrear las fuente IP de raíz del atacante porque literal cualquier dispositivo con IP diferente estará atacando el servidor. Y que pasa envía un poco de solicitudes al servidor haciendo que se pete y quede con un error 404 porque el servidor no lo soporto por culpa de esos BOTNET y eso hace que nosotros tengamos que pagar bastante por el consumo de la red que esta teniendo el servidor. Pero porque lo hacen con fin de dejar todo mal, pedir plata un rescate o algo peor.

CONSECUENCIAS

- El botnet comienza a **enviar tráfico masivo** al servidor web objetivo.
- Este tráfico puede parecer legítimo (peticiones HTTP, por ejemplo), pero su volumen es tan alto que **satura el servidor**.

Impacto en el servidor web

- El servidor no puede procesar todas las solicitudes y:
    - Se **ralentiza severamente**.
    - **Deja de responder** (caída del sitio).
    - Puede **colapsar la base de datos** si también es atacada o está enlazada con el sitio.

Tipo de Ataque	Descripción	Impacto
HTTP Flood	Inunda el servidor con peticiones HTTP GET o POST	Alto uso de CPU y RAM
SYN Flood	Envía solicitudes TCP incompletas que llenan las tablas de conexión	Saturación del sistema
UDP Flood	Envía paquetes UDP sin esperar respuesta	Consumo de ancho de banda
Slowloris	Mantiene muchas conexiones HTTP abiertas y lentas	Agota recursos del servidor web
Amplificación DNS/UDP	Usa servidores vulnerables para amplificar el tráfico hacia el servidor objetivo	Multiplica el volumen de ataque

SUPLANTACION DE IDENTIDAD (SPOOFING)

NIVEL DE AMENAZA: MEDIO

IMPACTO: ALTO

PROBABILIDADES: DIFICILES

RIESGO: PELIGROSO

El ataque podría ocurrir de muchas maneras en este caso hablemos de correos electrónicos pero como pongamos ejemplo Un usuario recibe un correo que aparenta ser de seguridad@empresa.com pidiendo que actualice su contraseña en un enlace falso. El enlace lleva a una página web falsa que roba las credenciales. El puede usar técnicas para hacerse pasar como de la empresa cambiando la dirección de correo el dominio o organización.

CONSECUENCIAS

El objetivo que tendrá para atacar es que obtendrá información sensible de ti desviar dinero o transferencia y junto descargar software alta mente peligroso o instalarte un spyware esos ataques son difíciles de contener

La solución es utilizar filtros antispam usar verificadores que puedan ver si esta autentico ese correo que te llega y no hacer clic porque das papaya porque ellos te pillan la IP enseguida.

Métodos	Descripción	Ejemplo
Phishing	Envío de correos falsos que suplantan a bancos, servicios en la nube, etc.	"Tu cuenta ha sido suspendida. Haz clic aquí para reactivarla."
Business Email Compromise (BEC)	Suplantación del CEO o financiero para solicitar transferencias urgentes.	"Juan, transfiere $10,000 a esta cuenta antes del cierre del día."
Spear Phishing	Phishing personalizado y dirigido a una persona clave.	"Hola Laura, revisa el informe del cliente XYZ que discutimos ayer."

Métodos	Descripción	Ejemplo
Domain Spoofing	Creación de dominios falsos similares al real.	empresá.com en lugar de empresa.com

✅ 3. Formación del Equipo de Respuesta a Incidentes

Objetivo: Definir un equipo de respuesta que pueda actuar de manera eficiente ante un incidente de seguridad.

Argumento: La existencia de un equipo estructurado reduce el tiempo de respuesta y mejora la coordinación durante un incidente, lo cual minimiza el impacto.

FORMACION DEL EQUPO DE RESPUESTA

ROLES	OCUPACION	LINEA DE CONTACTO
Coordinador de Seguridad	Es el que garantiza que opere de forma segura las operaciones de empresa cumpliendo con los reglamentos de la empresa	coordinadorSECURE@DEEL.com
SOPORTE TECNICO	Brinda ayuda y soporte alas fallas que se le presenten a los sistemas de una empresa para que pueda solucionarlo en el menor tiempo posible asegurando que el funcionamiento del sistema estén al 100% en operación.	Soporttecnico@DEEL.com
GERENTE	Su ocupación es el que toma las decisiones de cualquier novedad que le venga a su entidad y a sus servicios de la red.	GarenteDeelLA.corp@DELL.com

✅ 4. Desarrollo de Procedimientos de Detección

Objetivo: Implementar medidas para detectar amenazas antes de que causen daños mayores.

Argumento: La detección temprana permite contener incidentes antes de que escalen. Los logs y sistemas de alerta son esenciales en este proceso.

Componente	Descripción	Tipo de amenaza detectada	Ejemplo práctico	Herramientas comunes	Contribución a la detección temprana
Monitoreo de Logs	Revisión continua de registros del sistema, red y aplicaciones.	Accesos no autorizados, cambios sospechosos	Detección de múltiples intentos fallidos de login en un servidor web	Syslog, Logwatch, Graylog, Splunk, ELK Stack	Permite rastrear comportamientos anómalos desde su origen.
SIEM (Security Information and Event Management)	Correlación de eventos en tiempo real para detectar amenazas.	Intrusiones, movimientos laterales, malware	SIEM detecta patrones coincidentes con ransomware conocido	Splunk, IBM QRadar, ArcSight, AlienVault OSSIM	Analiza grandes volúmenes de datos para detectar amenazas complejas.
Alertas y Notificaciones Automáticas	Configuración de alertas ante eventos críticos.	Escaneos de red, tráfico inusual, cambios de configuración	Alerta por modificación de archivos del sistema sin autorización	Zabbix, Nagios, Wazuh, Microsoft Sentinel	Facilita una reacción inmediata ante incidentes en desarrollo.
Detección de Intrusos (IDS)	Inspección de tráfico de red en busca de patrones maliciosos.	Escaneos de puertos, exploits conocidos	Snort detecta un intento de explotación de	Snort, Suricata, Zeek (Bro)	Identifica amenazas antes de que comprometan

			Apache HTTP Server		sistemas críticos.
Análisis de comportamiento (UEBA)	Analiza el comportamiento de usuarios y entidades para detectar anomalías.	Cuentas comprometidas, actividad interna sospechosa	Usuario con permisos básicos accede a datos sensibles	Exabeam, Splunk UEBA, Securonix	Detecta amenazas internas y movimientos fuera del comportamiento normal.
Monitorización de Red (NTA)	Vigilancia constante del tráfico de red en busca de patrones extraños.	Ataques DDoS, comunicaciones con C2 (Command & Control)	Identificación de conexiones salientes a servidores en países sospechosos	Darktrace, Vectra AI, Corelight	Detecta amenazas que evaden los antivirus tradicionales.
Detección basada en firmas	Busca coincidencias exactas con patrones de malware conocidos.	Virus, gusanos, ransomware conocidos	Antivirus detecta un troyano identificado previamente	ClamAV, McAfee, Kaspersky, Sophos	Útil para detener amenazas conocidas de forma eficiente.
Detección basada en anomalías	Identifica comportamientos anormales aunque no coincidan con una firma específica	Zero-days, nuevas variantes de malware	Flujo de tráfico de red inusual durante la madrugada	OSSEC, Wazuh, CrowdStrike	Capta ataques nuevos o personalizados que no están en bases de datos de firmas.
Sandboxing	Ejecuta archivos sospechosos en entornos	Malware oculto, archivos	Análisis de un archivo adjunto de correo que	Cuckoo Sandbox,	Permite descubrir amenazas que se

	controlados para analizar su comportamiento	adjuntos maliciosos	ejecuta scripts maliciosos	FireEye, Joe Sandbox	ocultan tras archivos aparentemente inofensivos.
Detección en endpoints (EDR)	Monitorea en tiempo real los dispositivos finales (endpoints).	Keyloggers, ransomware, ataques dirigidos	Endpoint detecta ejecución de PowerShell sospechosa	CrowdStrike Falcon, SentinelOne, Microsoft Defender ATP	Permite detener ataques desde el punto de entrada antes de que se expandan.
Correlación de eventos múltiples	Asociación de eventos dispersos para identificar un patrón común de ataque.	Ataques avanzados persistentes (APT), campañas coordinadas	Login fallido + cambio de permisos + exfiltración de datos	SIEM, SOAR, ELK Stack	Reduce el tiempo de detección de ataques que escapan de los controles individuales.
Uso de listas negras / reputación IP	Bloqueo y alerta sobre direcciones IP o dominios maliciosos conocidos.	Phishing, C2, malware distribuidos por red	Conexión saliente a un dominio marcado como parte de una botnet	Spamhaus, VirusTotal, Threat Intelligence feeds	Evita conexiones y comunicaciones con fuentes ya reconocidas como peligrosas.
Honeypots	Sistemas trampa que simulan servicios vulnerables para atraer atacantes.	Escaneos automatizados, ataques de reconocimiento	Ataques a un servidor honeypot expuesto para recolectar IPs maliciosas	Cowrie, Dionaea, Honeyd	Permite estudiar el comportamiento del atacante sin riesgo real para el sistema.

✅ 5. Elaboración del Plan de Contención

Objetivo: Definir una serie de pasos para limitar el impacto de un incidente de seguridad.

Argumento: Un plan de contención bien estructurado reduce la propagación del daño y permite enfocar los recursos en la recuperación.

El plan que podríamos implementar para contrarrestar el problema de web:

1.Identificar el sistema que fue afectado y atacado viendo lo que es en los LOGS o Sistema de eventos y reportes y tomar lista.

2.Aislar el sistema dejarlo temporalmente fuera de servicio para revisar el daño que causo el atacante en el tema de los archivos y junto evitar la propagación de virus o troyanos que Allan instalado en el sistema.

3.Notificar de inmediato al equipo de respuesta para tomar accione para recuperar la información que fue perdida en el sistema en este caso bakups o respaldos alternos y juntos volverlos activar

4.Aumentar la seguridad en prioridad alta para prevenir otro nuevo incidente.

5.Hacer un análisis que podría haber causado la falla y junto ver si el atacante dejo puertas traseras o huellas o rastros digitales para tomar acciones urgentes.

✅ 6. Plan de Recuperación y Continuidad del Negocio

Objetivo: Establecer pasos para restaurar operaciones tras un incidente y continuar con el negocio.

Argumento: La continuidad del negocio es vital para mantener la confianza de los clientes y minimizar pérdidas financieras.

Ok los pasos que podríamos hacer en este tipo de situación para tener la información al instante sin perder tiempo son:

1.Verificar el sistema de respaldos si están en funcionamiento con el servidor donde se alojan porque en este caso si la victima no llego hacia esa parte si es que no lo logro se puede recuperar fácilmente, aunque claro esos respaldos se podrían alojar en servicios de almacenamiento virtual como DropBox,GoogleDrive Workspace o Microsoft.

2.Restuarar el sistema afectado en un sistema aislado de manera segura el tiempo puede depender dependiendo de la gravedad del daño que allá causado la víctima.

3.Realizar testeos para confirmar si ya todo esta funcionando como debe ser para que no allá ninguna amenaza e inicializar y cargar todo nuevamente.

4.Notificar a los clientes que hubo fallas en el servidor o exposición de datos para tomar acciones legales e investigación con las autoridades para encontrar el responsable encriptando la red del servidor y que este en monitoreo en todo momento.

5.Actualizar las normas y política en el tratamiento de datos.

✅ 7. Conclusiones y Reflexiones Finales

Este laboratorio nos enseño como tenemos que actuar en este tipo de incidente tomando ciertas acciones para detener este flagelo en la era digital por lo tanto hay muchas técnicas para detener el problema no pagando rescate ni nada fuera del estilo solo es saber como juegas con las cartas que tienes para ver cual de ellas es la que harás que ganes y puedas detener al atacante el diseño que hice fue para mí el más básico pero con eso podría bastar aunque hay otra formas pero ya seria para un después.