UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE INGENIERÍA
ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO

Examen Final
Caso: Cyber Breach at Target

RAFAEL ANDRÉS ALVAREZ MAZARIEGOS 1018419
XIMENA STEPHANIA ELIZARDI GOBERN 1101720
EDDIE ALEJANDRO GIRÓN CARRANZA 1307419
JULIO ANTHONY ENGELS RUIZ COTO 1284719
CÉSAR ADRIAN SILVA PÉREZ 1184519

GUATEMALA DE LA ASUNCIÓN, NOVIEMBRE DE 2024
CAMPUS CENTRAL “SAN FRANCISCO DE BORJA, S. J” DE LA CIUDAD DE GUATEMALA

Link de la presentación:
https://www.canva.com/design/DAGWIg76580/kcNipfcYqlComWXkN7GuNw/edit?utm_content=DAGWIg76580&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

Acciones inmediatas en respuesta al incidente

Un posible inicio sería movilizar al equipo de respuesta para proteger sistemas críticos y evitar que la amenaza se propague. Es esencial que los sistemas comprometidos se desconecten de la red para limitar el acceso a los atacantes, aplicando de inmediato restricciones en las cuentas y accesos sospechosos. Simultáneamente, el equipo de seguridad debe realizar una evaluación preliminar del incidente para determinar el alcance de los sistemas y datos comprometidos y establecer medidas de control que permitan retomar el control de la situación.
Igualmente es importante la notificación a la junta directiva y a los líderes de los departamentos clave, proporcionando una visión inicial del incidente y de las medidas de contención ya implementadas. A la par, es recomendable designar un portavoz interno temporal para centralizar la comunicación dentro de la organización y con el público, asegurando una respuesta coherente. Así también, es importante recabar información por medio de sistemas de monitoreo para detectar cualquier actividad sospechosa.
Y finalmente, un punto importante es la información de la situación a los empleados para que sepan lo sucedido y las acciones que se están tomando. Y de ser necesario informar a los clientes en general para evitar que el problema genere mala reputación.

1. Análisis de Riesgos
    a. Identificación de Activos Críticos
        i. Sistemas de Punto de Venta (POS): Los dispositivos y software que se utiliza para procesar transacciones de tarjetas de crédito y debido.
        ii. Redes Internas y Servidores: La infraestructura de las operaciones de ventas y almacenamientos de datos.
        iii. Bases de Datos de Clientes: Información personal y financiera de los clientes.
        iv. Sistemas de Seguridad de la Información: Herramientas y sistemas de detección de intrusos en nuestros sistemas.
        v. Identificación de Amenazas
    b. Amenas internas
        i. Falta de segmentación de la red
            1. Empleados no capacitados
            2. Amenazas externas
        ii. Ataques de malware
            1. Phishing a los proveedores y empleados
            2. Acceso no autorizado a través de terceros como con el proveedor Gazio Mechanical Services
            3. Evaluación de Vulnerabilidades
    c. Análisis Técnico
        i. Sistemas POS vulnerables sin actualizaciones de seguridad
            1. Evaluación de Procesos
        ii. Análisis de Probabilidad e Impacto

    d. Impacto en áreas potenciales
        i. Operacional con la interrupción de transacciones en tiendas
            1. Financiero en pérdidas de fraude y costos de recuperación
            2. Reputacional debido a la pérdida de confianza entre clientes y accionistas.
            3. Legal, en base a las demandas y sanciones regulatorias
2. Análisis de impacto en el Negocio
    a. Funciones y procesos Críticos
        i. Procesamiento de Transacciones
        ii. Protección de datos de clientes
        iii. Operaciones de tienda
        iv. Sistemas de comunicación interna
    b. Evaluación de impacto
        i. Operacional
            1. Interrupción en procesamientos de pagos
            2. Necesidad de operaciones manuales
            3. Retrasos y errores en el factor humano
        ii. Financiero
            1. Pérdida de ingresos por reducción de ventas
            2. Costos asociados a reembolsos
            3. Funcionalidad interrumpida en los POS
            4. Fallo de comunicación entre los dispositivos y su servidor
        iii. Reputacional
            1. Pérdida de confianza de los clientes
            2. Cobertura de los medios negativa
            3. Mala reputación de los hardware
        iv. Legal y Regulatorio
            1. Sanciones por incumplimiento de estándares de seguridad
    c. Priorización de funciones y sistemas
        i. Alta
            1. Restauración segura de sistemas de POS
            2. Protección y recuperación de bases de datos de clientes
            3. Restauración del control completo de nuestros sistemas
        ii. Media
            1. Fortalecimiento y recuperación de bases de datos de clientes
            2. Restablecimiento de comunicaciones seguras con proveedores
    d. Análisis de dependencias
        i. Técnicas: Sistemas POS dependen de la red y servidores con la seguridad de la información depende de herramientas como FireEye.
        ii. Operacionales: Operaciones de tienda depende de sistemas de transacciones funcionales relaciones con los proveedores que afectan en los suministros y servicios

3. Desarrollo del Plan de Continuidad del Negocio y Recuperación ante Desastres
    a. Identificación de Equipos y personal clave
        i. Equipo de gestión de crisis (CMT)
            1. Miembros

a. CEO
b. CIO
c. CISO
d. Directores Operacionales
e. Directores Legales
f. Directores de Comunicación

2. Responsabilidades
    a. Toma de decisiones estratégicas
    b. Coordinación general

ii. Equipo de respuestas a incidentes de TI (CIRT)

1. Miembros
    a. Especialistas en seguridad
    b. Ingeniero de redes
    c. Analistas de malware
    d. Director de TI
2. Responsabilidades
    a. Contención técnica
    b. Análisis de los sistemas
    c. Recuperación de sistemas

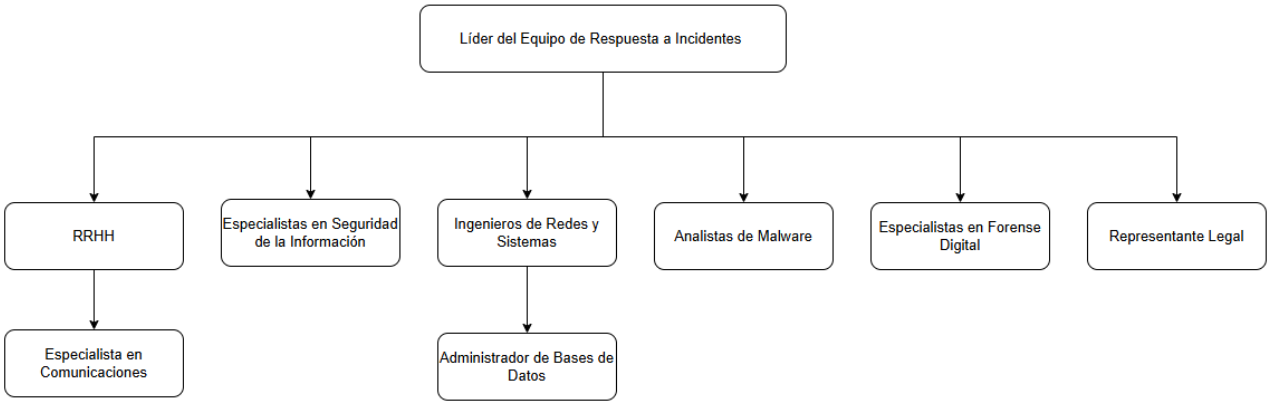
iii. Equipo de comunicación de crisis

1. Miembros
    a. Directores de comunicación
    b. Director de Relaciones públicas
    c. Recursos Humanos
2. Responsabilidades
    a. Gestión de comunicaciones internas y externas

b. Roles y responsabilidades
    i. Líder del CMT
    ii. Coordinador del CIRT
    iii. Portavoz Oficial

Perfiles esenciales

- Líder del Equipo de Respuesta a Incidentes
    - Coordina todas las actividades de respuesta al incidente.
    - Toma decisiones críticas sobre contención, erradicación y recuperación.
    - Sirve como punto de contacto principal entre el equipo técnico y la alta dirección.
- Especialistas en Seguridad de la Información
    - Monitorean alertas de seguridad y analizan eventos sospechosos.
    - Determinan el alcance e impacto del incidente.
    - Colaboran en la implementación de medidas de contención y mitigación.
- Ingenieros de Redes y Sistemas
    - Gestionan y aseguran la infraestructura de redes y sistemas.
    - Implementan acciones para aislar y restaurar sistemas afectados.
    - Revisan configuraciones y aplican parches de seguridad.



c. Procedimientos de recuperación

Actividades previas al incidente (preparación)

- Implementación de estrategias de mitigación
  - Tecnologías
    - Actualizar y parchear todos los sistemas y software de los POS y servidores.
    - Implementar segmentación de la red para aislar los sistemas críticos
    - Autenticación de dos factores para procesos remotos para los proveedores y empleados.
  - Procesos
    - Establecer protocolos claros de respuestas a incidentes
    - Realizar evaluaciones de seguridad periódicas
    - Pruebas de penetración
- Preparación de recursos
  - Contratos con proveedores
  - Capacitación

Actividades durante el incidente (respuesta inmediata)

- Activación del plan BC/DR
  - Basada en criterios de detección de malware en sistemas críticos o alertas de intrusión confirmadas
- Notificación y planificación
  - Comunicación interna
  - Comunicación externa
- Respuesta técnica
  - Aislamiento de sistemas afectados
    - Desconexión inmediata de sistemas comprometidos
      - Identificación rápida de los sistemas y dispositivos que han sido comprometidos o que muestran actividad sospechosa
      - Desconectar estos sistemas de la red para evitar la propagación del malware o acceso no autorizado

            - Desconexión de servidores, dispositivos y POS
        - Bloqueo de acceso no autorizado
            - Actualizar reglas de firewall para bloquea direcciones IP, dominios o puertos utilizados por los atacantes
            - Revocar las credenciales comprometidas y deshabilitar cuentas de usuario afectadas
    - Análisis y contención
        - Evaluación del alcance del incidente
        - Eliminación del programa maligno y amenazas
        - Aplicación de parches y actualizaciones de seguridad
        - Reforzamiento de medidas de seguridad
    - Restauración de sistemas
        - Restauración desde copias de seguridad seguras
            - Utilizar copias de seguridad recientes t verificadas que estén libres de malware y priorizar la restauración de sistemas críticos como las operaciones de los POS y bases de datos
        - Verificación de la integridad de los sistemas
            - Antes de reintegrar los sistemas la red, realizar pruebas exhaustivas para asegurar que estén libres de malware y funciones correctamente.
        - Reintegración gradual de la red
            - Reintroducir los sistemas a la red de manera controlada y monitoreada, supervisando de cerca el tráfico de red t actividades de los sistemas, por si hay alguna anomalía.
    - Medidas adicionales
        - Implementación de soluciones temporales
        - Monitoreo continuo
        - Comunicación con partes interesadas
- Continuidad de operaciones
    - Operaciones en tiendas
        - Implementar procedimientos manuales para el procesamiento de transacciones
        - Comunicación a los clientes sobre los posibles cambios o demoras de los sistemas
    - Soporte al cliente
        - Líneas de atención para clientes afectados
        - Información y medidas de monitoreo de crédito

d. Tareas y asignación de recursos

Equipo	Tareas y Asignación
TI	Priorizar la restauración de sistemas POS y bases de datos de los clientes, así como asegurar la implementación de controles de seguridad mejorados
Comunicación	Desarrollo de mensajes claros y transparentes para todas las partes interesadas, gestionando la reputación de la empresa durante y después del incidente
Legal y cumplimiento	Garantizar que todas las acciones cumplan con regulaciones y leyes aplicables coordinando con autoridades y organismos reguladores.

Manejo de comunicación ante incidentes.

Al tratarse de un ataque es fundamental que todas las partes interesadas estén enteradas y posean el mismo nivel de conocimiento sobre el inconveniente. La comunicación abierta y transparente es fundamental para no dar pasos a rumores y mantener la confianza de los clientes, a continuación, se proponen los enfoques ideales de comunicación para acercarse a clientes, empleados e inversionistas en caso de un ataque.

Una vez determinado el impacto del ataque, se debería de preparar en primer lugar la comunicación interna general con los empleados. Explicar de manera breve pero concisa el problema por el que se está atravesando junto con limitaciones y recomendaciones de seguridad. Establecer un canal interno (intranet, correo, o reuniones virtuales) donde los empleados puedan recibir actualizaciones frecuentes, así como una vía para resolver dudas.

A los socios y accionistas se les informará por medio de una comunicación inicial de alto nivel que explique el alcance del incidente y las medidas inmediatas que se han tomado. Se recomienda evitar tecnicismos excesivos y concentrarse en el impacto y en los planes de mitigación para preservar la confianza. Proveer informes periódicos sobre el progreso en la contención del incidente y los pasos de remediación que se estén implementando. Estas actualizaciones pueden enviarse a través de boletines especiales.

Finalmente, con los clientes se propone explicar qué tipo de datos podrían haberse visto afectados y, de ser necesario, ofrecer instrucciones sobre cómo monitorear sus cuentas o información personal. Establecer una línea de ayuda o página web específica para responder preguntas de los clientes y orientarlos sobre cualquier medida adicional que deban tomar. Brindar esta asistencia en un tono empático y accesible es clave. A medida que se implementan medidas de seguridad, comunicar estos esfuerzos a los clientes, demostrando el compromiso de la empresa con su seguridad y tranquilidad. Además, una vez resuelta la crisis, se puede enviar una actualización final explicando las lecciones aprendidas y mejoras realizadas en la infraestructura de ciberseguridad.

Mantener la transparencia y la confianza durante una crisis de ciberseguridad sin comprometer la seguridad de la información es un desafío que requiere una comunicación estratégica y cuidadosa. Para asegurar dichas características se recomienda evitar detalles técnicos muy complejos que puedan ser aprovechados por atacantes y en su lugar enfocar los comunicados a acciones generales que la empresa está tomando para resolver el problema.

Ser consistentes con la información otorgada es clave para evitar rumores o poder contradecirse y que el público en general dude de la veracidad de los comunicados, preparar guiones en conjunto y designar voceros ayuda a que la información dada al publico sea uniforme por todos los medios.

Dar actualizaciones sobre el estado del incidente cada cierto tiempo muestra transparencia, especialmente con los empleados, asegurarse de estén informados sobre cómo manejar consultas relacionadas con la crisis y proveer un canal de contacto dedicado para consultas externas reduce la posibilidad de filtraciones.

Por último, el limitar el acceso a información sensible únicamente a personal autorizado también evita que la información no sea distribuida sin control y nuevamente, filtraciones no deseadas.

Implementar un Programa Integral de Auditorías Internas y Externas

a. Auditorías Internas Regulares

- Frecuencia: Trimestral.
- Objetivo: Evaluar el cumplimiento de las políticas y procedimientos de seguridad internos.
- Acciones Específicas:
    - Establecer un equipo interno de auditoría de ciberseguridad multidisciplinario.
    - Utilizar marcos de referencia reconocidos (como NIST, ISO 27001) para guiar las evaluaciones.
    - Identificar y priorizar áreas de riesgo para una atención inmediata.

b. Auditorías Externas Independientes

- Frecuencia: Anual.
- Objetivo: Obtener una perspectiva imparcial sobre la eficacia de nuestras medidas de seguridad.
- Acciones Específicas:
    - Contratar a firmas especializadas en ciberseguridad de renombre.
    - Realizar pruebas de penetración y evaluaciones de vulnerabilidades.
    - Incorporar recomendaciones en planes de mejora continua.

Beneficios para la Organización:

- Mejora Continua: Identificación proactiva de debilidades y oportunidades de mejora.
- Cumplimiento Normativo: Asegurar el alineamiento con regulaciones y estándares de la industria.
- Confianza de Stakeholders: Demostrar transparencia y compromiso con la seguridad.

Realizar Simulacros y Ejercicios de Respuesta a Incidentes

a. Simulacros de Mesa (Tabletop Exercises)

- Frecuencia: Semestral.
- Objetivo: Evaluar la capacidad de respuesta de los equipos ante escenarios hipotéticos.
- Acciones Específicas:
    - Diseñar escenarios realistas basados en amenazas actuales.

    - Involucrar a todos los niveles organizativos, desde la alta dirección hasta el personal operativo.
    - Documentar acciones y decisiones para análisis posterior.

b. Ejercicios en Vivo (Live Drills)

- Frecuencia: Anual.
- Objetivo: Probar la efectividad de los planes de respuesta en condiciones controladas pero realistas.
- Acciones Específicas:
    - Simular ataques cibernéticos en entornos controlados.
    - Evaluar la coordinación entre departamentos y la eficacia de las comunicaciones.

Beneficios para la Organización:

- Preparación Mejorada: Fortalecer la capacidad de respuesta y recuperación ante incidentes reales.
- Identificación de Brechas: Detectar y corregir deficiencias en procedimientos y protocolos.
- Cultura de Seguridad: Fomentar la concienciación y el compromiso de los empleados.

Establecer Indicadores Clave de Desempeño (KPIs) en Seguridad Cibernética

A. Definición y Seguimiento de KPIs

- Tiempo Medio de Detección (MTTD): Medir la rapidez con la que se identifican las amenazas.
- Tiempo Medio de Respuesta (MTTR): Evaluar la eficiencia en la contención y mitigación de incidentes.
- Número de Incidentes Evitados: Cuantificar las amenazas neutralizadas antes de causar impacto.

B. Informes Periódicos a la Alta Dirección

- Frecuencia: Mensual.
- Objetivo: Mantener informada a la Junta Directiva sobre el estado de la seguridad y áreas de preocupación.
- Acciones Específicas:
    - Preparar reportes detallados con análisis de tendencias y recomendaciones.
    - Facilitar sesiones de revisión para discutir resultados y acciones estratégicas.

Beneficios para la Organización:

- Toma de Decisiones Informada: Utilizar datos objetivos para orientar inversiones y prioridades.
- Responsabilidad y Transparencia: Fomentar una cultura de rendición de cuentas en todos los niveles.
- Mejora Continua: Ajustar estrategias basadas en el desempeño real y cambios en el entorno de amenazas.

Incorporar Lecciones Aprendidas en los Planes de Continuidad del Negocio

A. Análisis Post-Incidente

- Objetivo: Extraer aprendizajes de cada incidente o simulacro para fortalecer los procesos.
- Acciones Específicas:
    - Conducir revisiones exhaustivas después de cada evento.
    - Documentar causas raíz, acciones tomadas y resultados obtenidos.
    - Actualizar políticas y procedimientos basados en los hallazgos.

B. Actualización Regular de los Planes de Continuidad

- Frecuencia: Anual o tras cualquier incidente significativo.
- Objetivo: Asegurar que los planes reflejen las mejores prácticas y el entorno actual.
- Acciones Específicas:
    - Revisar y ajustar estrategias de recuperación y comunicación.
    - Validar la efectividad de las soluciones tecnológicas y logísticas implementadas.
    - Involucrar a todas las partes interesadas en el proceso de actualización.

Beneficios para la Organización:

- Resiliencia Mejorada: Capacidad para adaptarse y recuperarse rápidamente de interrupciones.
- Reducción de Impacto: Minimizar las pérdidas operativas y financieras ante incidentes.
- Confianza Reforzada: Demostrar a clientes e inversores una gestión proactiva y responsable.

Lecciones aprendidas

Fortalecer la infraestructura de seguridad y monitoreo: Implementar herramientas de detección de amenazas avanzadas y garantizar que estas funciones operen con alertas configuradas de manera que generen una respuesta inmediata.
Las fallas en la detección de intrusiones en Target revelaron la importancia de contar con sistemas de monitoreo continuo y efectivos para una detección temprana de incidentes.

Asegurar segmentación de la red: La falta de segmentación en la red de Target permitió a los atacantes moverse a través de sistemas internos, accediendo a datos sensibles.
Mejorar la segmentación de red, aislando las áreas críticas, reduce el riesgo de que un intruso acceda a información delicada.

Optimizar los protocolos de respuesta ante incidentes: La experiencia de Target sugiere la necesidad de protocolos claros para cuando se detectan alertas críticas.
Esto incluye procedimientos para verificar, escalar y responder rápidamente a las alertas de seguridad, reduciendo el tiempo de respuesta y, por lo tanto, el impacto potencial.

Establecer comunicación eficaz con clientes y stakeholders: En Target la comunicación tardía y confusa con los clientes y la falta de coordinación con las instituciones financieras causaron desconfianza. Un plan de continuidad debería incluir estrategias de comunicación que mantengan a los clientes informados rápidamente y provean asistencia oportuna.

Mejorar la capacitación y asignación de responsabilidades: La estructura organizativa de seguridad debe incluir equipos de respuesta bien entrenados y responsabilidades claramente definidas, asegurando que los empleados respondan adecuadamente a las alertas de seguridad.