METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #22 COMPROMISO DE CORREO ELECTRÓNICO EMPRESARIAL

Directrices para manejar incidentes de compromiso de correo electrónico empresarial.

Autor IRM: CERT SG
Contribución: CERT a Dvens / Paloma Vargas
Versión del IRM: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

Traducción al Español

Paloma Amilene Vargas Alvarado
E-Mail: amilenhalvarado@gmail.com
Twitter / X: @AmileneVargas

CONTENIDO

1. ABSTRACTO

Esta Metodología de respuesta a incidentes es una guía rápida dedicada a los encargados de investigar un problema de seguridad específico.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

- Administradores.
- Centro de Operaciones de Seguridad.
- CISO y adjuntos.
- CERT (Equipo de respuesta ante emergencias informáticas).

Recuerda: Si enfrentas un incidente, sigue el IRM, toma notas. Mantén la calma y contacta inmediatamente al equipo de Respuesta a Incidentes o CERT de tu línea de negocio si es necesario.

2. PASOS PARA LA GESTIÓN DE INCIDENTES

SE DEFINEN 6 PASOS PARA GESTIONAR INCIDENTES DE SEGURIDAD

1. **Preparación**: prepárese para manejar el incidente
2. **Identificación**: detectar el incidente
3. **Contención**: limitar el impacto del incidente
4. **Remediación**: eliminar la amenaza
5. **Recuperación**: recuperarse a una etapa normal
6. **Lecciones aprendidas**: elaborar y mejorar el proceso

IRM proporciona información detallada para cada paso del proceso de respuesta a incidentes. Los pasos provienen de la Guía de Gestión de Incidentes de Seguridad Informática del NIST.

2.1 PREPARACIÓN

OBJETIVO: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, REUNIR INFORMACIÓN PARA AHORRAR TIEMPO DURANTE UN INCIDENTE.

- Desarrollar y aplicar políticas que aborden la seguridad del correo electrónico, los protocolos de autenticación (por ejemplo, SPF, DKIM, DMARC) y el uso aceptable.
- Integrar escenarios de BEC en los Planes de Respuesta a Incidentes, Guías de Procedimiento y Procedimientos más amplios, detallando roles, responsabilidades y pasos a seguir.
- Preparar un plan de comunicación para advertir a colaboradores, clientes o socios sobre ataques de BEC en curso.
- Establecer y mantener una lista de contactos para la eliminación de contenidos en proveedores de alojamiento, registradores de dominios y proveedores de servicios de correo electrónico.
- Ejecutar campañas periódicas de concienciación sobre BEC, ingeniería social, estafas e incidentes de phishing.
- Implementar una solución técnica que permita a los colaboradores reportar fácilmente correos electrónicos sospechosos a los equipos de seguridad o a un colaborador de seguridad perimetral.
- Crear canales dedicados, como direcciones de correo electrónico, perfiles en redes sociales y líneas telefónicas, para facilitar la denuncia externa de correos electrónicos sospechosos, llamadas telefónicas, transferencias fraudulentas y otros indicios de incidentes BEC.
- Establecer procedimientos específicos para el análisis de archivos adjuntos y enlaces URL en un entorno aislado o de otra manera seguro que impida la propagación de infecciones.
- Mantener una lista de contactos involucrados en transacciones financieras y transferencias bancarias, incluidos los validadores.
- Implementar procedimientos estrictos de verificación para transferencias bancarias y cambios de información de pago de proveedores.
- Establecer equipos interdisciplinarios de respuesta a incidentes y/o crisis con representantes de TI, seguridad, antifraude, comunicación, legal y unidades de negocio (agregar o excluir según la industria específica y las necesidades de su organización)

Monitoreo y Detección Automatizados

- Implementar monitoreo automatizado en todos los sistemas relevantes, incluidos los servidores de correo electrónico, los registros de acceso a la red y los sistemas de autenticación, para detectar continuamente indicadores de BEC.
- Asegurarse de que cualquier evento detectado genere una notificación inmediata al equipo de respuesta a incidentes para una investigación y acción rápidas.

- Utilizar herramientas de Gestión de Información y Eventos de Seguridad (SIEM) para correlacionar eventos e identificar de manera efectiva posibles patrones de BEC.

DEFINICIÓN: El compromiso de correo electrónico empresarial es un tipo de estafa financiera avanzada en la que los delincuentes utilizan el acceso comprometido a correos electrónicos para engañar a los empleados y que transfieran grandes sumas de dinero o información sensible. Los incidentes de BEC pueden resultar en pérdidas financieras significativas y daños a la reputación.

2.2 IDENTIFICACIÓN

OBJETIVO: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES APROPIADAS.

Identificación de indicadores de BEC

- Identificar correos electrónicos que soliciten transferencias bancarias, información sensible o cambios en los detalles de pago, especialmente aquellos con un tono urgente.
- Evaluar el impacto y la gravedad potencial del incidente según la naturaleza de la vulneración.
- Determinar el alcance de las cuentas comprometidas y la amplitud del ataque.
- Optar por utilizar sistemas de monitoreo centralizados en todas estas fuentes, de manera que cada detección genere una alarma para una reacción inmediata.
- Detectar correos electrónicos que transmitan sensación de urgencia, secreto o escenarios de alto riesgo para presionar a los destinatarios a tomar acciones rápidas sin una verificación minuciosa.
- Notar desviaciones en el tono, lenguaje o formato de los correos electrónicos de contactos conocidos o ejecutivos.
- Asegurarse de que las alertas sean entregadas instantáneamente al equipo de respuesta a incidentes y a las partes interesadas relevantes para facilitar una acción rápida.
- Evaluar los posibles impactos financieros, reputación y operativos según la naturaleza y el alcance del incidente de BEC.
- Definir niveles de severidad de acuerdo con el impacto potencial máximo en términos de pérdidas financieras, compromisos de datos y interrupciones operativas para priorizar los esfuerzos de respuesta y asignar recursos de manera efectiva.

Ampliando alcance

- Identificar todas las cuentas de correo electrónico que han sido comprometidas y evaluar el nivel de acceso que cada cuenta tenía dentro de la organización.
- Determinar cómo se ejecutó el incidente BEC, ya sea a través de phishing, toma de control de cuentas o aprovechando vulnerabilidades en la lógica empresarial.
- Identificar qué departamentos o unidades de negocio se ven afectados por el incidente BEC.
- Evaluar si el ataque se originó de una única fuente o de un grupo de actores de amenaza.

Involucrar a las partes apropiadas

- Al detectar un incidente de BEC, notifique de inmediato al personal de la empresa designado y autorizado para tomar decisiones críticas, como la alta dirección, los responsables de seguridad informática y los ejecutivos de finanzas.
- Asegúrese de que las decisiones sobre cómo actuar frente a correos electrónicos o transacciones fraudulentas se tomen de manera rápida, preferiblemente en minutos, para minimizar los posibles daños.
- Involucre a los departamentos pertinentes, incluidos TI, jurídico, relaciones públicas y finanzas, para garantizar una respuesta coordinada.
- Si es necesario, involucre a socios externos como proveedores de servicios de correo electrónico, empresas de ciberseguridad y organismos de aplicación de la ley para apoyar la investigación y los esfuerzos de mitigación.

Recolección de evidencia

- Recoja muestras de los correos electrónicos fraudulentos, asegurándose de que tanto los encabezados como el contenido del correo se conserven para su análisis. Analice los correos electrónicos fraudulentos recopilados para identificar patrones, como direcciones IP del remitente recurrente o enlaces maliciosos comunes.
- Asegúrese de que los encabezados del correo estén intactos para analizar el origen, la ruta y la autenticidad de los correos electrónicos.

2.3 CONTENCIÓN

OBJETIVO: MINIMIZAR LOS DAÑOS CAUSADOS POR EL INCIDENTE, PREVENIR ACTIVIDADES NO AUTORIZADAS ADICIONALES Y ASEGURAR LOS SISTEMAS Y CUENTAS COMPROMETIDOS PARA DETENER EL AVANCE DEL ATACANTE.

Gestión de la Comunicación

- Coordinarse con los equipos de relaciones públicas y legales para preparar declaraciones públicas o notificaciones apropiadas para los interesados, clientes y socios, al tiempo que se protege la información sensible.
- Colaborar con las agencias de seguridad desde las primeras fases de contención para ayudar en su investigación y seguir cualquier orientación que proporcionen.

Conservar pruebas para la investigación

- Asegúrese de que todos los registros relevantes (por ejemplo, registros del servidor de correo, registros de tráfico de red, registros de autenticación) se conserven en su formato original para análisis y como evidencia.
- Cree imágenes forenses de los sistemas comprometidos para ayudar en las investigaciones detalladas sin alterar la evidencia original ni manipular el hardware original.

Colaborar con las partes interesadas

- Establecer contactos con la entidad bancaria o financiera asociada respecto a los flujos de dinero para permitir procedimientos legales posteriores.
- Trabajar estrechamente con los equipos de TI, seguridad y otros equipos relevantes para implementar medidas de contención de manera efectiva y asegurar que todos los aspectos del incidente sean atendidos.
- Proporcionar actualizaciones regulares a los principales interesados sobre el estado de la contención y cualquier problema emergente.
- Coordinar con los proveedores de servicios de correo electrónico para bloquear correos maliciosos y proteger cuentas comprometidas.
- Comunicar la naturaleza fraudulenta de las campañas de correo electrónico comprometidas a las partes externas involucradas, como socios, clientes, instituciones financieras, etc.

Implementar mitigaciones a corto plazo

- Reducir temporalmente los privilegios de las cuentas que no son esenciales para los esfuerzos de contención con el fin de minimizar el riesgo de compromisos adicionales.
- Reforzar la supervisión en los sistemas y cuentas críticas para detectar cualquier actividad sospechosa durante la fase de contención.

Actualizar configuraciones de seguridad

- Aplique los parches y actualizaciones necesarios a los sistemas y software que puedan haber sido explotados durante el incidente de BEC.
- Ajuste las configuraciones de las herramientas y sistemas de seguridad para defenderse mejor contra las tácticas específicas utilizadas en el esquema actual de BEC.

2.4 REMEDIACIÓN (EXTERNA)

OBJETIVO: TOMAR MEDIDAS PARA ELIMINAR LA AMENAZA Y EVITAR INCIDENTES FUTUROS.

Si el contenido fraudulento está asociado con la estafa identificada y se aloja en línea:

- Identificar al propietario, proveedor de hosting y registrador de dominio del sitio fraudulento con documentación completa de la actividad maliciosa.
- Referenciar el sitio web fraudulento mediante barras de herramientas para bloqueo instantáneo en los principales navegadores web. Implementar el bloqueo a nivel empresarial a través de herramientas de seguridad en lugar de depender únicamente de las extensiones del navegador.
- Redactar una solicitud de abuso detallada explicando claramente la naturaleza del fraude identificado, proporcionando detalles y evidencia específicos. Incluir capturas de pantalla, encabezados de correos electrónicos, direcciones IP, marcas de tiempo y detalles de transacciones para agilizar una respuesta efectiva del registrador/proveedor de hosting.
- Enviar una solicitud de abuso a la empresa de hosting y registrador utilizando la dirección de correo establecida abuse@hostingcompany o abuse@registrar. Dar seguimiento mediante múltiples canales de comunicación, incluyendo sus equipos de respuesta de seguridad dedicados cuando estén disponibles.
- Dar seguimiento mediante contacto telefónico directo con los equipos de abuso/seguridad para agilizar el proceso y establecer un cronograma claro para la resolución.
- Reportar la cuenta de correo fraudulenta a la empresa de hosting de correo con una solicitud formal para la congelación o suspensión inmediata de la cuenta. Conservar la evidencia del correo electrónico de acuerdo con la política de retención de datos de su organización para posibles procesos legales.
- Presentar paquetes de evidencia completos incluyendo copias de correos electrónicos fraudulentos con encabezados completos, marcas de tiempo de accesos no autorizados y documentación del impacto financiero.
- Investigar y documentar todas las plataformas de redes sociales que estén siendo utilizadas por los actores de amenaza, incluyendo cuentas específicas, publicaciones y tácticas de mensajería.
- Presentar solicitudes coordinadas de eliminación en todas las plataformas de redes sociales afectadas con la información de contacto del equipo de seguridad de su organización para seguimiento.
- Bloquear toda la comunicación por correo electrónico hacia/desde la cuenta fraudulenta para prevenir acciones maliciosas.
- Si no se recibe respuesta o acción, dar seguimiento regularmente por correo electrónico y teléfono.

- Si el proceso de eliminación es lento o deficiente, considerar contactar a un equipo CERT local del país involucrado. Explicar los desafíos que ha estado enfrentando y solicitar su asistencia para resolver el problema. Proporcionar la evidencia aplicable.

2.5 REMEDIACIÓN (INTERNA)

OBJETIVO: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR INCIDENTES FUTUROS.

Implementar medidas inmediatas de seguridad de la cuenta, también conocidas como 'victorias rápidas'.

- Cambios de contraseña obligatorios para todas las cuentas afectadas y potencialmente afectadas.
- Implementación de autenticación multifactor para todas las cuentas de correo electrónico empresarial.
- Revisión y revocación de reglas de reenvío de correo sospechosas.
- Suspensión de protocolos de correo electrónico antiguos que puedan eludir los requisitos de MFA.

Realizar un escaneo exhaustivo del entorno de correo electrónico para mejorar la alerta temprana de incidentes de BEC.

- Reglas de reenvío de correo no autorizadas
- Reglas sospechosas en la bandeja de entrada que mueven, eliminan o reenvían mensajes automáticamente
- Permisos de acceso de delegados inusuales
- Evidencia de ex filtración de correos electrónicos o descarga masiva

Implementa soluciones avanzadas de seguridad de correo electrónico con capacidades mejoradas.

- Detectar ubicaciones y horarios de inicio de sesión anómalos
- Identificar patrones sospechosos de reenvío
- Señalar comportamientos inusuales de envío
- Poner en cuarentena los mensajes con indicadores de BEC

Implementar protocolos estrictos de autenticación de correo electrónico.

- DMARC, también conocido como Autenticación de Mensajes Basada en Dominio, Reportes y Conformidad
- SPF, también conocido como Marco de Políticas del Remitente
- DKIM, también conocido como Claves de Dominio en el Correo Electrónico Identificado

- Configurar, si se considera aceptable, políticas para rechazar, en lugar de simplemente poner en cuarentena, los mensajes que fallan.

Establecer salvaguardias financieras de emergencia.

- Implementar pasos de verificación adicionales temporales para todas las transacciones financieras.
- Mantener en espera cualquier transacción pendiente hasta que se completen los procesos de verificación.
- Implementar verificación fuera de banda para todos los cambios de pago y transferencias electrónicas.
- Establecer flujos de aprobación basados en umbrales que requieran múltiples autenticadores.

Desplegar sistemas de monitoreo de transacciones para una detección mejorada.

- Destinos o montos de pago inusuales.
- Cambios en la información bancaria de proveedores establecidos.
- Solicitudes financieras urgentes o con alta presión.
- Transacciones que se desvían de los patrones establecidos

2.6 RECUPERACIÓN

OBJETIVO: RESTAURAR LOS SISTEMAS Y SERVICIOS AFECTADOS A SU OPERACIÓN NORMAL, ELIMINAR LAS CAUSAS RAÍZ DEL INCIDENTE, FORTALECER LAS MEDIDAS DE SEGURIDAD PARA PREVENIR OCURRENCIAS FUTURAS Y ASEGURAR QUE LA ORGANIZACIÓN SE HAYA RECUPERADO COMPLETAMENTE DEL COMPROMISO.

Análisis de causa raíz.

- Analizar todos los detalles de las fases de Identificación y Contención para entender cómo ocurrió el incidente de BEC.
- Determinar los métodos y vectores específicos utilizados por los atacantes, como correos electrónicos de phishing, malware o credenciales comprometidas.
- Identificar cualquier configuración incorrecta o brecha de seguridad que haya sido explotada durante el ataque.

Análisis del Impacto Financiero.

- Evalúe el impacto financiero determinando la magnitud de la pérdida.
- Determine el impacto en la información sensible, las transacciones financieras y la integridad operativa.
- Contacte a las instituciones financieras relevantes para informar sobre el fraude.
- Solicite la reversión de cualquier transacción no autorizada si se considera posible.
- Ponga temporalmente en modo de solo lectura las cuentas afectadas para evitar un acceso no autorizado adicional.

Erradicación de la amenaza.

- Escanee y limpie todos los sistemas afectados para eliminar malware, software espía u otro software malicioso introducido durante el ataque.
- Identifique y elimine cualquier cuenta de usuario o servicio no autorizado creado por los atacantes.
- Elimine cualquier puerta trasera, script o proceso automatizado instalado para facilitar el acceso continuo.

Parchear Vulnerabilidades

- Aplica parches y actualizaciones a todo el software, sistemas operativos y aplicaciones para cerrar vulnerabilidades explotadas.
- Ajusta las configuraciones del sistema para cumplir con las mejores prácticas de seguridad y minimizar las debilidades explotables.

Mejorar la seguridad del correo electrónico.

- Implementar o actualizar soluciones de seguridad de correo electrónico con funciones avanzadas de protección contra amenazas, como sandboxing y heurísticas avanzadas.
- Aplicar cifrado para las comunicaciones de correo electrónico sensibles para proteger los datos en tránsito

Implementar medidas avanzadas de autenticación.

- Ampliar la implementación de MFA en todas las cuentas de usuario, especialmente en aquellas con acceso a sistemas críticos.
- Aplicar políticas de contraseña seguras, incluyendo requisitos de complejidad y cambios de contraseña periódicos

Mejoras en la seguridad de la red.

- Desplegar o actualizar los controles de seguridad aplicables (WAF, IDS, IPS, etc.) para monitorear y bloquear actividades maliciosas en tiempo real.
- Segmentar aún más las redes para limitar el acceso entre diferentes unidades organizativas y reducir la superficie de ataque.

Estrategias de Protección de Datos y Copias de Seguridad.

- Asegúrese de realizar copias de seguridades regulares y seguras de los datos críticos y almacenarlas sin conexión o en un entorno de nube seguro.
- Implemente soluciones DLP para monitorear y proteger los datos sensibles contra el acceso no autorizado o la ex filtración.

Restaurar desde copias de seguridad limpias.

- Restaurar datos y sistemas a partir de copias de seguridad verificadas para estar libres de compromisos, asegurando que los datos restaurados sean precisos y estén actualizados.
- Confirmar que todos los sistemas restaurados funcionen correctamente y de manera segura, sin amenazas residuales

Volviendo a las operaciones normales.

- Pruebe y valide todos los servicios y sistemas para asegurarse de que funcionan según lo esperado después de la restauración.
- Restablezca gradualmente el acceso de los usuarios a los sistemas, asegurándose de que todas las cuentas sean seguras y estén autorizadas.

Informe a los interesados.

- Proporcione informes detallados a las partes interesadas relevantes sobre el proceso de remediación y su efectividad.
- Cumpla con cualquier requisito legal o normativo de informes relacionado con el incidente de BEC, asegurando transparencia y cumplimiento.

Comunicación y conciencia.

- Desarrollar capacitación específica en concienciación sobre seguridad enfocada en la prevención del BEC.
- Implementar procedimientos de verificación adicionales para transacciones financieras y comunicaciones.
- Establecer protocolos de comunicación claros para futuros incidentes de seguridad.
- Realizar ejercicios regulares de simulación de phishing enfocados en escenarios de BEC.
- Proporcionar capacitación dedicada al personal de finanzas y contabilidad sobre detección de fraude.

2.7 LECCIONES APRENDIDAS

OBJETIVO: DOCUMENTE LOS DETALLES DEL INCIDENTE, DISCUTA LAS LECCIONES APRENDIDAS Y AJUSTE LOS PLANES Y DEFENSAS.

Informe.

Un informe de crisis debe redactarse y estar disponible para todos los actores de la célula de gestión de crisis.

Se deberán describir los siguientes temas:

- Causa inicial de la infección
- Acciones y cronogramas de cada evento importante
- ¿Qué salió bien?
- ¿Qué salió mal?
- Costo del incidente
- Indicadores de compromiso

Capitalizar.

- Considerar qué pasos de preparación podría haber tomado para responder al incidente más rápido o de manera más eficiente.
- Actualizar sus listas de contactos y agregar notas sobre cuál es la forma más efectiva de contactar a cada parte involucrada.
- Considerar qué relaciones dentro y fuera de su organización podrían ayudarle con futuros incidentes.
- Mejorar los filtros DKIM, SPF y DMARC.
- Colaborar con los equipos legales si se requiere una acción legal.

3. DEFINICIONES

CONCEPTO	DESCRIPCIÓN
IRM	Metodología de Respuesta a Incidentes
CISO	Chief Information Security Officer (ejecutivo responsable de la seguridad de la información)
CERT	Equipo de Respuesta a Incidentes Informáticos
NIST	Instituto Nacional de Estándares y Tecnología
Business Email Compromise (BEC)	Es un tipo de estafa financiera avanzada en la que los delincuentes utilizan el acceso a correos electrónicos comprometidos para engañar a los empleados y lograr que transfieran grandes sumas de dinero o información sensible.
SPF (Sender Policy Framework)	Marco de políticas del remitente para validar qué servidores pueden enviar correos en nombre de un dominio.
DKIM (DomainKeys Identified Mail)	Método de autenticación mediante firmas criptográficas para verificar que el correo no fue alterado.
DMARC (Domain-based Message Authentication, Reporting & Conformance)	Sistema que utiliza SPF y DKIM para dar instrucciones a los receptores sobre cómo manejar correos que fallan la autenticación (ej. rechazar o poner en cuarentena).
Indicadores de Compromiso (IoC)	Elementos técnicos como direcciones IP de remitentes recurrentes, enlaces maliciosos o patrones de comportamiento que identifican un ataque.
Encabezados de Correo (Email Headers)	Datos técnicos del mensaje que deben preservarse intactos para analizar el origen, el enrutamiento y la autenticidad del correo.
Análisis de Sandbox	Entorno seguro y aislado donde se ejecutan archivos adjuntos o se analizan URLs para evitar que una posible infección se propague a la red principal.
MFA (Multi-Factor Authentication)	Autenticación de múltiples factores; capa de seguridad adicional requerida para acceder a cuentas críticas.

SIEM (Security Information and Event Management)	Herramientas utilizadas para correlacionar eventos de seguridad e identificar patrones de BEC de manera efectiva.
DLP (Data Loss Prevention)	Soluciones para monitorear y proteger datos sensibles contra el acceso o la ex filtración no autorizada.
Reglas de Buzón (Mailbox Rules)	Configuraciones en la cuenta de correo que los atacantes suelen crear para redirigir, mover o borrar mensajes automáticamente y así ocultar su actividad.
Takedown	Imágenes Forenses: Copias bit a bit de sistemas comprometidos que permiten realizar investigaciones detalladas sin alterar la evidencia original.
Imágenes Forenses	Copias bit a bit de sistemas comprometidos que permiten realizar investigaciones detalladas sin alterar la evidencia original.
Segregación de Red	Acción de aislar sistemas afectados de la red principal para evitar el "movimiento lateral" de los atacantes hacia otras áreas de la organización.