METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #15 INFRACCIÓN DE MARCA REGISTRADA

Directrices para manejar y responder a incidentes de infracción de marcas.

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 hoja de consulta dedicada a los encargados que investigan un problema preciso de seguridad.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

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

Recuerde: Si se enfrenta a un incidente, siga el IRM y tome notas. **Mantenga la calma** y, si es necesario, contacte inmediatamente con el equipo de Respuesta a Incidentes o el CERT de su línea de negocio.

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.

- Mantener una lista de todas las marcas registradas legítimas pertenecientes a su empresa y sus filiales. Esto ayudará a evaluar la situación actual y evitará que inicie un procedimiento de infracción sobre una marca registrada desactualizada, o sobre un sitio web o cuenta de red social legítima no relacionada.
- Establecer una lista de información completa y basada en evidencia relacionada con sus marcas para respaldar sus derechos legales:
    - Nombre(s), dominios legítimos y cuentas de redes sociales utilizadas por su empresa y sus filiales.
    - Palabras, símbolos, slogans, gráficos, etc., registrados como marca
    - Número(s) de registro de la marca, si corresponde.
    - Oficinas de registro de marcas internacionales y federales/locales (USPTO, INPI, etc.) donde las marcas registradas hayan sido etiquetadas como tales, si corresponde
    - Cualquier otro documento que demuestre claramente que una marca pertenece a su empresa.
- Preparar formularios de correo electrónico para infracción de marcas. Los usará en cada caso de infracción de marca, de ser posible en varios idiomas. Esto ayudará a agilizar el proceso al tratar de comunicarse con el registrador, proveedor de servicios y cualquier otra parte relevante durante el procedimiento.
- Promover un sistema centralizado de gestión de dominios utilizando campos WHOIS normalizados.
- Promover una publicidad en línea ética para evitar aparecer en dominios aparcados.
- Preparar procesos y plantillas de eliminación con el equipo legal.
- Contar con procesos, expertos y tecnologías para gestionar el portafolio de marcas.
- Tener un proceso centralizado o repositorio para gestionar nombres de marca aplicables, PI, dominios, información personal (PII), palabras clave, etc.

Contactos internos

- Mantener una lista de todas las personas involucradas en el registro de marcas en la empresa, especialmente las que forman parte de los departamentos legal y de relaciones públicas.
- Mantener una lista de todas las personas acreditadas para tomar decisiones sobre marcas y acciones eventuales relacionadas con la infracción de

marcas. Si es posible, obtener un acuerdo por escrito que le otorgue la capacidad de tomar este tipo de decisiones.

Contactos externos.

- Establecer y mantener una lista de contactos externos dentro de los registradores y proveedores de servicios involucrados en cuestiones de marcas.

2.2 IDENTIFICACIÓN

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

Detección de Infracción de Marca.

- Desplegar monitoreo activo del registro de nombres de dominio a través de las actualizaciones de las zonas de los registros siempre que sea posible o mediante servicios de alertas de marca.
- Configurar fuentes para monitorear nombres de usuario, páginas y grupos en redes sociales.
- Analizar los referidores HTTP en los registros del sitio web para identificar descargas de contenido fraudulentas y la duplicación fraudulenta de tus sitios web.
- Configurar monitoreo del nombre de la marca con motores de búsqueda especializados.
- Aprovechar la automatización siempre que sea posible para activar alarmas y mejorar los tiempos de reacción.
- Recopilar y analizar alertas de socios de confianza.

Involucrar a las partes adecuadas.

- Tan pronto como se detecte una infracción, contactar a las personas en tu empresa que estén acreditadas para tomar una decisión si no se te ha facultado para hacerlo por tu cuenta.

La decisión de actuar sobre el nombre de dominio fraudulento, grupo o cuenta de usuario debe tomarse lo antes posible.

Recopilar evidencia.

- Recopilar evidencia de nombres de dominio infractores, sitios web, URLs específicas (por ejemplo, URL personalizada de Facebook), páginas, grupos o detalles de cuentas.
- Hacer una copia con sello de tiempo del material infractor (página, grupo, blog, foro, línea de tiempo de microblogging, etc.) y tomar capturas de pantalla si es posible

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

Evalúa el impacto de la infracción de marca:

- ¿Puede utilizarse para redirigir el tráfico (cybersquatting, typosquatting, SEO)?
- ¿Puede utilizarse para suplantación, falsificación o estafas (cybersquatting con redirección al sitio web corporativo)?
- ¿Puede utilizarse para difamar la marca?
- Evalúa la visibilidad del componente infractor:
  - Visibilidad del sitio web (posicionamiento).
  - Número de seguidores o fans en redes sociales.
- Monitorea el dominio infractor inactivo en busca de señales de actividades fraudulentas.

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA DETENER LA INFRACCIÓN DE MARCAS.

En la mayoría de los casos relacionados con marcas registradas, la vigilancia suele ser suficiente. La remediación solo debe iniciarse si hay un impacto en su empresa o en sus subsidiarias.

Nombre de dominio.

- Contacte al propietario del nombre de dominio y al proveedor de servicios de alojamiento para notificarles sobre la infracción de la marca registrada y solicitarles que eliminen el contenido fraudulento.
- Contacte al registrador del nombre de dominio para notificarle sobre la infracción de la marca registrada y pedirle que desactive el nombre de dominio asociado o que lo transfiera a usted.
- Solicite al propietario del nombre de dominio o al registrador que redirijan todas las solicitudes DNS a sus servidores de nombres si es posible.
- Si ni el propietario del nombre de dominio ni el registrador cumplen con sus solicitudes, inicie un procedimiento de la Política Uniforme de Resolución de Disputas de Nombres de Dominio (UDRP) si está autorizado para hacerlo o pida a los contactos internos que lo lleven a cabo.

Cuenta en red social.

- Contacte al proveedor de servicios de la página, grupo o cuenta infractora para notificarle sobre cualquier violación de sus Políticas de Marca Registrada o Términos de Servicio y solicite que desactiven la cuenta infractora.
- Solicite al proveedor de servicios transferir la cuenta de la marca registrada a una cuenta de empresa existente si es posible.

En ambos casos, envíe correos electrónicos a las direcciones de contacto del registrador o proveedor de servicios. Generalmente hay una dirección de correo electrónico para reportar abusos, problemas legales o de derechos de autor.

Complete un formulario de queja por marca registrada o abuso si está disponible.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Evaluar el final del caso.

- Asegurarse de que el nombre de dominio, página, grupo o cuenta infractora estén desactivados o redirigidos a su empresa.
- Continuar monitoreando el nombre de dominio, página, grupo o cuenta infractora. A veces un sitio web puede reaparecer más tarde.
- Considerar la adquisición del nombre de dominio infractor si está disponible.

2.6 LECCIONES APRENDIDAS

OBJETIVO: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR LOS PLANES Y LAS DEFENSAS.

Informe

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores del incidente.

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

- Considera qué pasos de preparación, podrías haber tomado para responder al incidente más rápido o de manera más eficiente.
- Actualiza tus listas de contactos y agrega notas sobre cuál es la forma más efectiva de contactar a cada parte involucrada.
- Considera qué relaciones dentro y fuera de tu organización podrían ayudarte con futuros incidentes.
- Colabora 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 Emergencias Informáticas.
SOC (Centro de Operaciones de Seguridad)	Usuarios previstos de estas guías que investigan problemas de seguridad precisos.
USPTO / INPI	Oficinas de registro de marcas federales, locales o internacionales (como la Oficina de Patentes y Marcas de EE. UU. o el Instituto Nacional de la Propiedad Industrial) donde se validan los derechos legales de una empresa.
Registrador de Dominios (Registrar)	Entidad con la que se debe contactar para solicitar la desactivación o transferencia de un dominio infractor.
Campos WHOIS	Datos técnicos de registro de dominios; las fuentes sugieren normalizarlos mediante un sistema central de gestión para facilitar la administración.
Referentes HTTP (HTTP referrers)	Datos en los registros (logs) de un sitio web que permiten identificar descargas de contenido fraudulento o la creación de sitios "espejo".
Sitio Espejo Fraudulento (Fraudulent mirroring)	Duplicación no autorizada de un sitio web legítimo para engañar a los usuarios.
Nombres de Dominio Aparcados (Parked domain names)	Dominios registrados que no tienen contenido activo; las fuentes recomiendan evitar publicidad en ellos para mantener la ética de la marca.
Servidores de Nombres (Name servers)	Servidores técnicos a los que se puede solicitar que se redirijan las peticiones DNS de un dominio infractor una vez recuperado.
Ciberocupación (Cybersquatting)	Registro de dominios que usurpan una marca para redirección de tráfico o estafas.
Typosquatting	(Información externa) Registro de dominios con errores ortográficos comunes de una marca para

	capturar tráfico de usuarios que escriben mal la URL; las fuentes lo identifican como un impacto de la infracción.
SEO (Optimización en Motores de Búsqueda)	Uso de la marca infractora para manipular los resultados de búsqueda y redirigir el tráfico hacia sitios no autorizados.
Vanity URL	Direcciones personalizadas en redes sociales (como las de Facebook) que deben ser recolectadas como evidencia si infringen la marca.
UDRP (Política Uniforme de Resolución de Disputas de Nombres de Dominio)	Procedimiento legal y técnico que se inicia cuando el dueño o registrador de un dominio no accede a las peticiones de baja voluntaria.
Takedown (Baja de contenido)	Proceso de preparación de plantillas y acciones para eliminar contenido que viola los términos de servicio o políticas de marca de un proveedor.
IoC (Indicadores de Compromiso)	Evidencias técnicas del incidente que deben documentarse en el reporte final para ajustar las defensas futuras.
PII (Información de Identificación Personal)	Datos que deben ser gestionados de forma centralizada junto con los activos de marca.