MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

GUIA DE ACCIÓN ANTE INCIDENTES DE SPAM

PROCESO DE GESTIÓN DE INCIDENTES

Octubre - 2023

TABLA DE CONTENIDO

Concepto de Spam: Envío masivo y no deseado de correos electrónicos.

Detalles: Los mensajes de spam suelen ser enviados de forma indiscriminada a una gran cantidad de destinatarios, la mayoría de los cuales no han dado su consentimiento para recibirlos. En general dichos mensajes tienen una finalidad comercial, aunque puede haberlos que contengan algún tipo de malware.

El spam se caracteriza por ser contenido no solicitado y, en muchos casos, promociona productos o servicios comerciales, ofertas fraudulentas, campañas de marketing engañosas, contenido de naturaleza cuestionable o incluso intentos de estafas y phishing. Los remitentes de spam suelen utilizar técnicas automatizadas para recopilar direcciones de correo electrónico y otras formas de información de contacto, incluso compran o alquilan listas de contactos.

Impacto: el spam no solo puede ser molesto y abrumador para los destinatarios, sino que también puede representar un riesgo para la seguridad. Los enlaces o archivos adjuntos incluidos en los mensajes de spam pueden contener malware o llevar a sitios web maliciosos diseñados para robar información personal o financiera.

1. Fase de Identificación

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciber incidente que pueda sufrir un organismo o entidad, y notificarlo a la brevedad para tomar acciones ante el incidente.

- ✓ Identificar qué persona o personas han sufrido el spam.
- ✓ Comprobar las direcciones de correo electrónico para verificar la procedencia de los mensajes.
- ✓ Notificar al equipo de respuesta a incidentes de seguridad (CSIRT) de la organización o al equipo de seguridad de la empresa.
- ✓ Comunicar internamente con los equipos pertinentes, como el equipo de tecnología de la información, para coordinar la respuesta y garantizar una acción rápida.
- ✓ Notificar a los usuarios afectados y proporcionar instrucciones sobre cómo manejar los correos electrónicos no deseados y evitar caer en trampas de phishing o malware asociadas.

2. Fase de Contención

La máxima prioridad en esta fase es contener el impacto negativo que pueda sufrir la organización a causa del defacement.

Evaluación de la situación

- ✓ Obtener toda la información posible sobre el ataque: o Realizar una copia del correo electrónico sospechoso, manteniendo las cabeceras.
- ✓ Tomar evidencias gráficas, como capturas de pantalla de las páginas sospechosas.
- ✓ Analizar el contenido del mensaje de spam y evaluar si existe algún riesgo adicional, como enlaces maliciosos o archivos adjuntos infectados.
- ✓ Examinar los registros de correo electrónico, registros del servidor web y cualquier otro registro o archivo relevante para obtener más información.
- ✓ Determinar el alcance del incidente de spam.
- ✓ Documentar y recopilar todas las pruebas disponibles, como copias de los correos electrónicos no deseados, información de los encabezados de los correos y cualquier otro dato relacionado.
- ✓ Realizar copias de respaldo de la evidencia recopilada para su posterior análisis y referencia.

Contención

- ✓ No descargar ni ejecutar ningún archivo adjunto sospechoso.
- ✓ Tratar de contactar con el "emisor" mediante un medio alternativo conocido, empleando datos de contacto confiables (correo electrónico, teléfono de contacto, etc.).

3. Fase de Mitigación

- ✓ Una vez recopilada y analizada la información obtenida en la fase de contención, deben tomarse medidas reactivas para gestionar el incidente.
- ✓ Identificar los sistemas o cuentas de correo electrónico involucrados en el envío de spam y tomar medidas para detener la actividad no deseada.
- ✓ Bloquear o restringir los dominios o direcciones IP utilizados por los remitentes de spam, para evitar la propagación.
- ✓ Interactuar con los proveedores de servicios de correo electrónico para informar sobre el incidente y solicitar el bloqueo de los dominios o direcciones involucrados.
- ✓ Actualizar los filtros de correo y las reglas de detección de spam para prevenir futuros incidentes similares.
- ✓ Realizar un análisis forense de los sistemas y las cuentas involucradas para identificar cómo se originó el envío de spam y si hay alguna vulnerabilidad explotada.

- ✓ Examinar los registros del servidor de correo, los registros de acceso y cualquier otro registro o archivo relevante para obtener más información sobre la fuente y los métodos utilizados por los atacantes.

En caso de que algún usuario de la organización haya ejecutado o abierto un archivo adjunto

- ✓ Aislar el dispositivo.
- ✓ Notificar al equipo de sistemas de la organización para que realicen labores de investigación y desinfección.
- ✓ En caso de sospecha sobre credenciales comprometidas, restablecerlas y asegurar que los usuarios utilicen contraseñas fuertes y únicas

4. Fase de Recuperación

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante buscar cualquier signo de actividad sospechosa en los servicios afectados y monitorizarlos temporalmente.

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante buscar cualquier signo de actividad sospechosa en los servicios afectados y monitorizarlos temporalmente.

- ✓ Limpiar y restaurar las cuentas de correo electrónico afectadas, eliminando cualquier contenido no deseado y restaurando la funcionalidad normal.
- ✓ Realizar una revisión exhaustiva de las medidas de seguridad existentes, como autenticación del correo electrónico, filtros de spam y sistemas de detección de intrusiones.
- ✓ Proporcionar educación y capacitación en seguridad para los empleados para aumentar la conciencia sobre los riesgos asociados con el spam.

5. Fase Post- Incidente

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

6. Lecciones aprendidas

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del

problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

- ✓ Realizar una revisión post-incidente para identificar las lecciones aprendidas y las áreas de mejora en las políticas y prácticas de seguridad.
- ✓ Actualizar las políticas y procedimientos de seguridad de la organización en base a los hallazgos del incidente.
- ✓ Proporcionar capacitación y concienciación en seguridad a los empleados para prevenir futuros incidentes de spam.

7. Diagrama de flujo