SKILLS INNOVATION
DESARROLLANDO HABILIDADES

Pasos clave a seguir en caso de que tu organización haya sido víctima de un ciberataque

1.Detectar el incidente:

Utiliza sistemas de detección de intrusos, monitoreo de registros y herramientas de seguridad para identificar la actividad sospechosa o inusual en la red o sistemas.

2. Aísla y contiene el ataque:

Una vez detectado el ataque, es importante tomar medidas inmediatas para aislar y contener la amenaza. Esto puede implicar desconectar sistemas comprometidos o cerrar el acceso a la red.

3. Notifica a las Autoridades

En algunos casos, especialmente si se trata de un ataque cibernético importante, es necesario notificar a las autoridades locales o agencias gubernamentales de ciberseguridad.

4. Notifica a los Afectados Internos

Informa a los miembros internos relevantes de la organización sobre el incidente, incluidos los equipos de seguridad, gerencia y personal de TI.

5. Evalúa el Alcance y el Daño

Realiza una evaluación exhaustiva del alcance del ciberataque y el daño potencial. Esto puede incluir la pérdida de datos, la interrupción de servicios y la identificación de la vulnerabilidad explotada.

6. Restablece la Seguridad

Identifica y corrige las vulnerabilidades explotadas y restablece la seguridad de los sistemas y la red. Esto podría incluir la aplicación de parches de seguridad y cambios en las contraseñas.

7. Restauración de Datos

Si se perdieron datos, utiliza las copias de seguridad para restaurar la información perdida y verificar su integridad.

8. Reanuda las Operaciones

Trabaja en la recuperación de sistemas y servicios para reanudar las operaciones normales lo antes posible. Esto puede requerir la restauración de sistemas desde copias de seguridad.

9. Comunicación Externa

Notifica a los clientes, socios comerciales y otras partes externas afectadas por el incidente de seguridad. Proporciona información precisa y transparente sobre lo sucedido y las medidas que estás tomando.

10. Evaluación Post-Incidente

Realiza una revisión exhaustiva del incidente una vez que se haya resuelto. Analiza lo que salió mal y cómo se puede mejorar la postura de seguridad.

11. Mejoras de Seguridad

Implementa medidas de seguridad adicionales o mejoradas basadas en las lecciones aprendidas del incidente.

12. Informe a las Autoridades

En muchos países, la ley requiere la notificación de incidentes de seguridad cibernética a las autoridades de protección de datos. Cumple con las obligaciones legales pertinentes.

13. Educación y Concientización Continua

Refuerza la educación y la concientización en seguridad cibernética entre los empleados para evitar futuros incidentes.

14. Preservación de Evidencia

Si es necesario, conserva evidencia digital que pueda ser útil en investigaciones futuras o acciones legales contra los atacantes.

15. Contratación de Expertos en Ciberseguridad

Si es necesario, considera la contratación de expertos en ciberseguridad o servicios de respuesta a incidentes para ayudar en la investigación y mitigación del ataque.