Informe de Incidente de Ciberseguridad. Análisis de Incidente de Acceso no Autorizado

1. Resumen Ejecutivo

- **Descripción del Incidente:**
  Esta mañana, una pasante reportó que no podía acceder a su cuenta de red interna. Sin embargo, los registros de actividad muestran que su cuenta accedió recientemente a la base de datos de clientes. La pasante mencionó haber recibido un correo electrónico solicitándole que accediera a un sitio web externo para recuperar un mensaje utilizando sus credenciales de red. Se sospecha que este método de phishing fue utilizado por un atacante para obtener acceso a la red interna y a la base de datos de clientes. Además, se ha observado que varios registros de clientes han sido eliminados o manipulados.

2. Fase de Identificación

- **Acción Realizada:**
  El equipo de gestión de incidentes llevó a cabo una auditoría completa de los sistemas afectados, dispositivos y políticas de acceso. Tras el análisis, se descubrió que el atacante utilizó las credenciales robadas de la pasante para acceder a la base de datos de clientes. Se confirmaron manipulaciones en los datos, lo que incluyó la eliminación de ciertos registros.
- **Impacto Inicial:**
  Algunos datos de los clientes fueron comprometidos, eliminados o modificados. Esto supone una exposición crítica de información confidencial y un riesgo para la integridad de los datos.

3. Fase de Protección

- **Acciones Implementadas:**
  1. Autenticación Multifactor (MFA):
     Se ha implementado MFA para fortalecer la seguridad en los accesos a la red interna.
  2. Limitación de Intentos de Inicio de Sesión:
     Ahora se limitan los intentos de inicio de sesión a tres intentos fallidos para evitar futuros ataques de fuerza bruta.
  3. Capacitación del Personal:
     Se ha iniciado una formación obligatoria para todos los empleados sobre la protección de sus credenciales de inicio de sesión, específicamente contra ataques de phishing.

4. Refuerzo de la Infraestructura de Seguridad:
   Implementación de un firewall más robusto y planificación para instalar un Sistema de Prevención de Intrusiones (IPS) que detecte y bloquee intentos de intrusión.

4. Fase de Detección

- **Monitoreo Continuo:**
  - El equipo ha puesto en marcha un Sistema de Detección de Intrusiones (IDS) para monitorear todo el tráfico de red entrante y detectar comportamientos sospechosos en tiempo real.
  - Se emplearán herramientas de registro avanzado para auditar continuamente los accesos y cualquier actividad anómala en la red.

5. Fase de Respuesta

- **Medidas Inmediatas:**
  1. Desactivación de la Cuenta Comprometida:
     La cuenta de la pasante ha sido deshabilitada inmediatamente para prevenir nuevos accesos no autorizados.
  2. Notificación a la Gerencia y Clientes:
     La alta dirección ha sido informada del incidente y se contactará a los clientes afectados a través de correo electrónico para notificarles sobre la brecha de seguridad.
  3. Reporte a las Autoridades:
     De acuerdo con las regulaciones locales, se informará a las autoridades pertinentes y a las organizaciones reguladoras sobre la filtración de datos.

6. Fase de Recuperación

- **Restauración de Datos:**
  - Los datos eliminados serán restaurados utilizando la copia de seguridad completa de la base de datos de la noche anterior. Todo el personal ha sido informado de que deberán volver a ingresar la información modificada o añadida durante esta mañana una vez que el proceso de restauración finalice.
  - Se ha establecido un plan de verificación para asegurar la integridad de los datos después de la restauración y validar que no se omita ninguna información importante.

7. Recomendaciones y Lecciones Aprendidas

- Fortalecimiento de la Autenticación:
  La autenticación multifactor y la capacitación continua son medidas clave para prevenir incidentes futuros.
- Implementación de Políticas de Seguridad más Rígidas:
  Limitar el acceso a la información crítica mediante controles más estrictos y auditorías regulares de accesos.
- Comunicación y Concienciación:
  Se requiere una mayor sensibilización entre los empleados sobre el riesgo de phishing y la importancia de reportar correos electrónicos sospechosos de inmediato.