**Plan de Respuesta a Incidente de Ransomware basado en NIST**

**Identificación**

Activos afectados:

* Servidor de archivos: Documentación interna, operaciones diarias.
* Base de datos de clientes: Información personal, financiera y confidencial.
* Sistemas de backup: Copias de seguridad críticas.

Vulnerabilidades detectadas:

* Falta de segmentación de red: Todos los sistemas, incluyendo backups, estaban en la misma red.
* Falta de EDR o antivirus con protección activa.
* Falta de concienciación sobre ciberseguridad para los empleados.
* No se utilizó MFA ni controles de acceso robustos.

**Protección**

Medidas preventivas recomendadas:

* Segmentación de red: Separar entornos de producción, backup y estaciones de trabajo.
* Seguridad en endpoints: Implementación de EDR y antivirus con capacidad de respuesta automática.
* Control de acceso: Aplicación de principios de privilegio mínimo y MFA.
* Políticas de seguridad:
  + Política de uso correcto del correo electrónico.
  + Restricciones de ejecución de archivos ejecutables en correos.
  + Gestión segura de contraseñas.
* Capacitación continua en ciberseguridad para todos los empleados.
* Actualizaciones y parches regulares para todos los sistemas y software.

**Detección**

Métodos y herramientas:

* SIEM (Gestión de información y eventos de seguridad) para centralizar logs y encontrar eventos sospechosos.
* Sistemas IDS/IPS para monitoreo de tráfico de red y detección de eventos maliciosos.
* EDR con capacidad de detección de ejecución de ransomware y aislamiento del endpoint.
* Monitoreo del correo electrónico con sandboxing para archivos adjuntos.

Protocolo de alerta temprana:

Configurar alertas automáticas en caso de:

* Acceso inusual a documentos.
* Actividades de cifrado masivo.
* Conexiones inusuales.

Establecer canales de reporte rápido para que empleados informen eventos sospechosos.

**Respuesta**

Plan de acción al detectar un ataque:

Contención inmediata:

* Aislar sistemas infectados de la red.
* Bloquear tráfico malicioso a través del firewall.
* Desactivar cuentas comprometidas.

Análisis del incidente:

* Determinar el alcance y los vectores de entrada.
* Identificar los sistemas y datos comprometidos.

Notificación:

* Interna: Informar a todas las partes relevantes.
* Externa: Notificar a clientes afectados si es necesario y autoridades regulatorias.

Comunicación pública:

* Designar un portavoz oficial.
* Preparar mensajes para prensa y clientes, sin divulgar detalles técnicos sensibles.

|  |  |  |
| --- | --- | --- |
| Rol | Responsable | Funciones |
| Coordinador de Incidentes | Lider de TI o CISO | Coordinar la respuesta, activar el plan y reportar los avances |
| Equipo Técnico | Administradores de Sistemas | Contención, restauración y análisis forense |
| Legal y Compliance | Asesor Legal | Evaluar las implicaciones legales, reportar entidades |
| RR.HH y Capacitación | Departamento de RR.HH | Reforzar políticas internas y acciones correctivas |

**Recuperación**

Pasos de recuperación:

* Verificar la erradicación completa del malware.
* Restaurar sistemas desde backups seguros y no comprometidos.
* Restablecer accesos de forma gradual y segura.
* Actualizar todas las contraseñas y claves de acceso.
* Aplicar todos los parches de seguridad pendientes.
* Monitorización reforzada de los sistemas por al menos 30 días post-recuperación.

Plan de continuidad del negocio:

* Mantener operaciones críticas en servidores en la nube seguros o fuera de la red comprometida.
* Establecer canales de atención alternativos para clientes.
* Priorizar la restauración de servicios esenciales.

**Mejora Continua**

* Realizar un informe completo del incidente: causas, impacto, tiempos de respuesta, errores y aciertos.
* Realizar una reunión de lo aprendido.
* Actualizar políticas, herramientas y procedimientos según lo sucedido.
* Simular escenarios similares cada 6 meses como parte de ejercicios de ciberseguridad.
* Indicadores clave de desempeño:
  + Tiempo de detección.
  + Tiempo de contención.
  + Tiempo de recuperación.
  + Nivel de participación del personal.