**Análisis de Vulnerabilidades – Terra Renewables**

**Tabla de Vulnerabilidades Identificadas**

| **Tipo de Vulnerabilidad** | **Vulnerabilidad Explotada** | **Descripción** |
| --- | --- | --- |
| Proceso | Monitoreo de Seguridad Inadecuado | Monitoreo solo en horario laboral (8:00-17:00), permitiendo incidentes sin detección fuera de horario. |
| Proceso | Falta de Segregación de Funciones | Transferencia de 3.5M€ realizada sin verificación adicional por un empleado de tesorería. |
| Tecnología | Gestión Inadecuada de Accesos Remotos | Credenciales de acceso remoto expuestas en redes sociales debido a controles insuficientes. |
| Tecnología | Falta de Segregación de Redes | Sin segregación de redes, facilitando movimientos laterales por parte de atacantes. |
| Personas | Falta de Concienciación en Seguridad | Empleado subcontratado expuso credenciales sensibles en redes sociales. |
| Personas | Falta de Verificación en Comunicaciones | Transferencia financiera ejecutada sin verificar autenticidad del correo del CEO. |
| Proceso | Gestión de Incidentes Reactiva | Demora en análisis del incidente del 25 de julio hasta el día siguiente. |
| Tecnología | Falta de Protección contra Phishing | Ausencia de controles efectivos ante correos de phishing, facilitando un ataque exitoso. |

**Análisis de Impacto**

| **Tipo de Impacto** | **Descripción** |
| --- | --- |
| Impacto Financiero | Riesgo potencial de pérdida de 3.5M€ y costos operativos adicionales por investigaciones posteriores. |
| Impacto en la Reputación | Daño a la confianza de clientes y socios, percibiendo vulnerabilidad a ciberataques. |
| Impacto Operacional | Interrupción de operaciones normales, intervención de altos directivos, recursos adicionales requeridos para resolución. |
| Impacto Legal y de Cumplimiento | Posibles violaciones a regulaciones como GDPR, con riesgos de sanciones regulatorias. |
| Impacto en Seguridad Informática | Compromiso de información sensible creando vectores adicionales para ataques futuros. |

**Controles Recomendados**

| **Tipo de Control** | **Control** | **Descripción** |
| --- | --- | --- |
| Preventivo | Implementación de Autenticación Multifactor (MFA) | Aplicar MFA para accesos remotos y sistemas críticos. |
| Preventivo | Sistema de Monitoreo Continuo 24/7 | Sistema de monitoreo permanente con alertas automáticas. |
| Preventivo | Política de Segregación de Funciones | Doble aprobación requerida para transacciones significativas. |
| Detectivo | Sistema Anti-Phishing Avanzado | Soluciones IA para detección y bloqueo efectivo de phishing. |
| Correctivo | Plan de Respuesta a Incidentes Mejorado | Procedimientos claros, tiempos definidos, roles específicos y simulacros periódicos. |
| Preventivo | Programa de Concienciación en Seguridad | Formación continua en seguridad, simulaciones regulares y formación específica. |

**Cuadro de Mando para el Comité de Dirección**

| **Métrica** | **Descripción** | **Definición de límites** |
| --- | --- | --- |
| Tiempo Medio de Detección (MTTD) | Tiempo promedio desde inicio hasta detección de incidentes. | Verde: <1 hora Ámbar: 1-4 horas Rojo: >4 horas |
| Tasa de Éxito en Simulaciones de Phishing | Porcentaje de empleados que no caen en simulaciones trimestrales de phishing. | Verde: >90% Ámbar: 75-90% Rojo: <75% |
| Cobertura de MFA | Porcentaje de sistemas críticos con MFA implementado. | Verde: >95% Ámbar: 80-95% Rojo: <80% |
| Tiempo Medio de Respuesta (MTTR) | Tiempo promedio en contener y resolver incidentes. | Verde: <2 horas Ámbar: 2-8 horas Rojo: >8 horas |
| Índice de Vulnerabilidades Críticas | Vulnerabilidades críticas o altas sin parchear en sistemas críticos. | Verde: 0 Ámbar: 1-3 Rojo: >3 |

**Acciones de Comunicación y Concienciación**

| **Tipo de Acción** | **Acción** | **Descripción** |
| --- | --- | --- |
| Comunicación | Comunicado a Clientes Afectados | Comunicado personalizado a clientes afectados explicando incidente, acciones correctivas y contacto directo para dudas. |
| Comunicación | Comunicado Interno de Transparencia | Sesión informativa con empleados sobre incidentes, lecciones aprendidas y nuevas medidas de seguridad. |
| Concienciación | Programa de Formación en Seguridad Digital | Formación obligatoria con talleres prácticos, simulaciones mensuales de phishing, formación específica por área y evaluaciones periódicas. |