Caso de Estudio

TechSolutions

CC Diego Cabuya

MY Sergio Cruz

MY Víctor López

MY Yerson Torres

TechSolutions

- Desarrollo de software y servicios en la nube
- Base de clientes masiva
- Vasta cantidad de datos sensibles
- Su infraestructura de TI es compleja

CASO:

Es el 10 de junio de 2025. Su equipo como expertos en ciberseguridad ha detectado una serie de actividades anómalas

ESTRATEGIA DE **DEFENSA EN PROFUNDIDAD** INTEGRAL

OBJETIVOS

Mitigar el impacto del incidente

Proteger a la empresa contra futuros ataques

TechSolutions

PROCESO

1. Análisis de Amenazas y Vulnerabilidades
2. Principios de Defensa en Profundidad
3. Capas de Defensa Propuestas
4. Respuesta al Incidente
5. Monitoreo y Mejora Continua

MITRE ATT&CK™

Cyber Kill Chain

ISO

27005

Gestión de riesgos de seguridad de la información

27035

Gestión de Incidentes de Seguridad

CASO - SECUENCIA DEL CIBERATAQUE

TechSolutions

Fase del Caso	Descripción	Etapas del Cyber Kill Chain
Fase 1: Vectores de Ataque Iniciales	- Phishing a empleados - Exploit de día cero en servidor web público - Archivo malicioso desde LinkedIn	**1. Reconocimiento:** Probable análisis previo de empleados y sistemas vulnerables **2. Armamento:** Creación de malware/correo y exploit **3. Entrega:** Phishing, archivo, exploit
Fase 2: Movimiento Lateral y Persistencia	- Uso de credenciales robadas - Escaneo interno de red - Elevación de privilegios - Creación de cuentas ocultas y tareas maliciosas	**4. Explotación:** Uso efectivo del phishing/exploit **5. Instalación:** Persistencia mediante cuentas/tareas **6. Comando y Control (C2):** Posible canal interno o beaconing
Fase 3: Exfiltración / Destrucción	- Acceso a base de datos de propiedad intelectual en la nube - Tráfico de exfiltración a IPs externas - Ransomware y cifrado de archivos	**7. Acciones sobre Objetivos:** Exfiltración de datos, cifrado, destrucción parcial del entorno

Amenaza	Táctica MITRE	Técnica MITRE	Clasificación ISO/IEC 27005	Tipo de Origen	Activos Afectados	Descripción
Phishing dirigido a empleados	Acceso inicial	T1566.001 – Spearphishing Attachment	Amenaza humana externa (ingeniería social / suplantación)	Externo	Usuarios / Cuentas de correo	Envío de correos con adjuntos maliciosos para robar credenciales.
Descarga de archivo malicioso desde LinkedIn	Acceso inicial	T1204.002 – Malicious File	Amenaza humana externa (ingeniería social / malware en canales sociales)	Externo	Usuarios / Estaciones de trabajo	El usuario descarga un archivo infectado desde red social profesional.
Explotación de vulnerabilidad de día cero en servidor DMZ	Ejecución / Explotación	T1203 – Exploitation for Client Execution	Amenaza técnica externa (explotación de vulnerabilidad técnica)	Externo	Servidor en DMZ / Aplicaciones web	El atacante explota una vulnerabilidad no parcheada en servidor.
Uso de credenciales robadas	Acceso persistente	T1078 – Valid Accounts	Amenaza humana externa (uso indebido de credenciales)	Externo	Sistema de autenticación / red interna	Se utilizan credenciales válidas para acceder a la red.
Escaneo de red interna	Descubrimiento	T1046 – Network Service Scanning	Amenaza técnica interna (reconocimiento / descubrimiento no autorizado)	Interno (tras compromiso)	Topología de red / Inventario de hosts	El atacante escanea servicios/hosts para reconocer el entorno.

Amenaza	Táctica MITRE	Técnica MITRE	Clasificación ISO/IEC 27005	Tipo de Origen	Activos Afectados	Descripción
Elevación de privilegios	Elevación de privilegios	T1068 – Exploitation for Privilege Escalation	Amenaza técnica interna (apropiación de privilegios)	Interno (tras compromiso)	Sistemas críticos / Control de acceso	Aprovecha vulnerabilidad o privilegios para ganar control avanzado.
Creación de cuentas ocultas y tareas programadas	Persistencia	T1053.005 – Scheduled Task/Job: Scheduled Task	Amenaza técnica interna (persistencia encubierta)	Interno (tras compromiso)	Configuración de sistemas / Políticas de tareas	Crea cuentas ocultas y modifica tareas para mantenerse en el sistema.
Exfiltración de datos hacia IPs desconocidas	Exfiltración	T1041 – Exfiltration Over C2 Channel	Amenaza técnica externa (exfiltración de información confidencial)	Externo	Bases de datos / Repositorios de código	Extrae datos sensibles a través de canales externos no autorizados.
Cifrado de archivos y nota de rescate (ransomware)	Impacto	T1486 – Data Encrypted for Impact	Amenaza técnica externa (destrucción de información / ransomware)	Externo	Archivos sensibles / Disponibilidad de servicios	Cifra archivos importantes y deja instrucciones de rescate.

Vulnerabilidad	Clasificación ISO/IEC 27005	Tipo de Activo Afectado
Conciencia débil de los usuarios ante amenazas sociales	Vulnerabilidad humana (concienciación insuficiente)	Recursos Humanos / Usuarios
Software desactualizado en servidor DMZ (sin parchear)	Vulnerabilidad técnica (parcheo/configuración)	Infraestructura TI (servidores en DMZ)
Falta de segmentación y control del movimiento lateral	Vulnerabilidad técnica (arquitectura de red)	Red y comunicaciones internas
Ausencia de controles sólidos sobre privilegios y cuentas	Vulnerabilidad técnica y organizacional (gestión de privilegios)	Control de accesos / Sistemas de autenticación
Monitoreo inadecuado de tráfico saliente y comportamiento	Vulnerabilidad técnica (monitoreo y respuesta)	Sistemas de monitoreo / Red de datos
Protección débil de datos críticos en la nube	Vulnerabilidad técnica (protección de datos)	Datos sensibles / Repositorios cloud
Backups no resilientes ni segmentados ante *ransomware*	Vulnerabilidad técnica (respaldo y recuperación)	Infraestructura de backup / almacenamiento
Ausencia de autenticación multifactor en accesos críticos	Vulnerabilidad técnica (autenticación)	Sistemas críticos / Consolas de acceso
Gestión ineficiente del ciclo de vida de cuentas y accesos	Vulnerabilidad organizacional (gestión de identidades y accesos)	Sistemas de Gestión de Identidad y Acceso/ Recursos Humanos

Principio	Descripción General	Aplicación en el Caso
Capas múltiples	Establecer varias líneas de defensa que operen de forma coordinada y redundante.	El phishing y el malware ingresaron porque fallaron simultáneamente el filtrado de correo, la capacitación y la autenticación MFA.
Segmentación y contención	Dividir la red en zonas seguras para evitar desplazamientos no autorizados.	El atacante logró escanear y moverse lateralmente en la red por falta de segmentación adecuada y control de acceso interno.
Mínimo privilegio	Limitar el acceso de usuarios y servicios solo a los recursos estrictamente necesarios.	La persistencia fue posible por permisos elevados y cuentas mal gestionadas.
Seguridad desde el diseño	Integrar la seguridad desde la arquitectura y desarrollo de sistemas.	El servidor en la DMZ con software desactualizado refleja una ausencia de diseño seguro y validación previa al despliegue.
Supervisión y respuesta continua	Monitorear, detectar y responder en tiempo real a incidentes de seguridad.	La exfiltración de datos no fue detectada a tiempo, evidenciando un SOC o SIEM con baja cobertura o correlación.
Resiliencia y redundancia	Establecer mecanismos de respaldo, recuperación y continuidad operativa.	El ransomware afectó sistemas críticos sin respaldo inmutable ni recuperación estructurada.
Concienciación del usuario	Formar y sensibilizar continuamente al personal sobre amenazas y buenas prácticas.	El usuario comprometido por phishing y la descarga maliciosa en LinkedIn reflejan una débil cultura de ciberseguridad.

Capa de Defensa en Profundidad	Objetivo de la Capa	Medidas de Seguridad	Tecnologías Clave
Capa 1: Perímetro / Red Externa	Evitar accesos no autorizados desde el exterior y contener amenazas entrantes.	NGFW, WAF, IDS/IPS, SEG, ZTNA, filtrado de tráfico, hardening de servidores públicos.	Fortinet, Palo Alto, Cloudflare WAF, Zscaler, Proofpoint, Azure Firewall.
Capa 2: Red Interna / Segmentación	Limitar el movimiento lateral y contener el compromiso en zonas específicas.	Segmentación por VLAN, firewalls internos, microsegmentación, control de tráfico este-oeste.	Cisco ISE, Illumio, Guardicore, Azure NSG, Vectra AI, Darktrace.
Capa 3: Endpoint / Dispositivos	Proteger y monitorear los dispositivos utilizados por usuarios y técnicos.	EDR/XDR, parches automáticos, hardening de sistemas, control de puertos y USB, MDM.	CrowdStrike, SentinelOne, Microsoft Defender, Intune, Tanium.
Capa 4: Aplicaciones	Blindar el desarrollo, despliegue y uso de software ante técnicas de explotación.	SDLC seguro, pruebas SAST/DAST, DevSecOps, control de sesiones, cifrado en tránsito.	SonarQube, Veracode, GitHub/GitLab Secure, AWS WAF, Azure App Defender.
Capa 5: Datos	Proteger la confidencialidad, integridad y disponibilidad de la información.	Clasificación de datos, cifrado, DLP, respaldos inmutables, políticas de retención y auditoría.	Microsoft Purview, AWS KMS, Veeam, Cohesity, OneTrust, BigID.
Capa 6: Identidad y Acceso	Garantizar que solo identidades autorizadas accedan a recursos definidos.	MFA, acceso condicional, RBAC/ABAC, gestión de privilegios (PAM), detección de anomalías.	Azure AD, Okta, CyberArk, BeyondTrust, Microsoft Entra, IAM integrado en cloud.
Capa 7: Operaciones y Concienciación	Desarrollar una cultura organizacional resiliente y capacidad de respuesta continua.	SOC 24/7, SIEM, SOAR, plan de respuesta a incidentes, simulacros, campañas de concienciación.	Splunk, Microsoft Sentinel, Cortex XSOAR, KnowBe4, Red Canary, ISO/IRP templates.

Fase del Proceso (ISO/IEC 27035)	Descripción General	Aplicación en el Caso
1. Preparación	Establecimiento de políticas, procedimientos, roles y capacidades para la respuesta a incidentes.	Activación del plan IRP, conformación del equipo IRT, coordinación con proveedores cloud y de seguridad.
2. Identificación	Detección, análisis y confirmación de eventos como incidentes de seguridad.	Confirmación de phishing, tráfico anómalo hacia IPs externas, ransomware y acceso a bases de datos sensibles.
3. Evaluación	Análisis del alcance, naturaleza e impacto del incidente sobre los activos de la organización.	Clasificación del incidente como crítico por afectación a propiedad intelectual, sistemas de desarrollo y riesgo reputacional.
4a. Contención	Acciones inmediatas para evitar que el incidente se propague o afecte a otros sistemas.	Aislamiento de estaciones y sistemas comprometidos, bloqueo de cuentas y tráfico sospechoso, segmentación de zonas críticas.
4b. Erradicación	Eliminación completa de la causa raíz del incidente y limpieza de componentes comprometidos.	Eliminación de malware, reversión de configuraciones alteradas, eliminación de cuentas ocultas, parcheo de vulnerabilidades.
4c. Recuperación	Restauración segura de los servicios afectados y validación de su integridad.	Restauración desde respaldos inmutables, reinstalación de sistemas comprometidos, pruebas de integridad antes del reintegro.
5. Lecciones Aprendidas	Análisis retrospectivo del incidente para mejorar procesos, controles y respuesta futura.	Reconstrucción del ataque, análisis de causas, revisión de políticas, y retroalimentación al sistema de defensa en profundidad.

Área de Mejora Continua	Acciones Propuestas	Relación con el Incidente Analizado
Revisión de capacidades de detección	Fortalecer SIEM, implementar reglas de correlación avanzadas y sensores en entornos cloud y endpoints.	La exfiltración de datos y persistencia no fueron detectadas oportunamente.
Actualización de procedimientos IRP	Ajustar guías de contención, roles y flujos de comunicación para mejorar la respuesta ante ransomware y APTs.	El procedimiento fue activado, pero no fue lo suficientemente ágil frente al ataque multifase.
Análisis post-mortem estructurado	Implementar sesiones formales de revisión tras incidentes críticos, con documentación y seguimiento.	Lecciones aprendidas deben integrarse a futuras simulaciones y formación.
Integración de inteligencia de amenazas	Establecer fuentes de CTI (Cyber Threat Intelligence) y alianzas con CSIRTs sectoriales.	No se anticiparon indicadores de compromiso ni tácticas del atacante antes del incidente.
Entrenamiento y simulacros periódicos	Realizar ejercicios TTX (Tabletop Exercise) e híbridos simulando escenarios de compromiso similares y progresivos.	El phishing y el ransomware evidencian que los usuarios y el equipo técnico no estaban lo suficientemente entrenados.
KPIs de resiliencia y respuesta	Establecer métricas para evaluar tiempos de detección, contención, erradicación y recuperación.	Se requiere medir la mejora operativa post incidente para validar la madurez del sistema de defensa en profundidad.
Retroalimentación al SGSI	Actualizar políticas, controles y evaluación de riesgos como parte del ciclo PDCA del SGSI.	El incidente reveló vulnerabilidades no contempladas en el análisis previo y brechas en controles documentados.

TechSolutions

GRACIAS