ESCUELA SUPERIOR
DE GUERRA
"General Rafael Reyes Prieto"
Colombia

TechSolutions

- MY. Luis Alberto Chavarro Gutiérrez
- MY. Diego Esmeral Madrid
- MY. Alex Guerrero Cortes
- MY. Edna Robles Ocampo

Que ocurrió?

El 10 de junio de 2025, TechSolutions Corp., una empresa global líder en software y servicios en la nube, fue víctima de un ciberataque avanzado en tres fases. El ataque comenzó con correos de phishing sofisticados, explotación de una vulnerabilidad de día cero en un servidor en la DMZ, y la ejecución de malware desde redes sociales. Posteriormente, los atacantes lograron moverse lateralmente por la red, escalar privilegios y establecer persistencia en el entorno, con el objetivo final de exfiltrar datos confidenciales y desplegar ransomware.

Análisis de Amenazas y Vulnerabilidades

Fase 1 - Vectores de Ataque Iniciales

- Phishing dirigido a empleados simulando comunicaciones del departamento de TI.
- Explotación de vulnerabilidad de día cero en servidor web obsoleto ubicado en la DMZ.
- Malware descargado desde redes sociales a través de archivos adjuntos falsos.

Fase 2 - Movimiento Lateral y Persistencia

- Compromiso de una estación de trabajo mediante credenciales robadas.
- Escaneo interno de red y escalamiento de privilegios.
- Creación de cuentas ocultas y tareas programadas maliciosas.

Fase 3 - Exfiltración / Destrucción

- Robo de datos críticos (propiedad intelectual y código fuente).
- Tráfico saliente inusual hacia IPs no reconocidas.
- Infección por ransomware en servidores clave.

Principios de Defensa en Profundidad

Cada capa debe ser independiente y complementaria, abarcando desde el perímetro de la red hasta la concienciación del usuario.

Principios clave:

- Redundancia de controles.
- Diversidad de tecnologías y enfoques.
- Minimización de la superficie de ataque.
- Detección y respuesta rápida.
- Educación y concienciación continua.

Principios de Defensa en Profundidad

Capa 1: Perímetro / Red Externa

- Principio aplicado: Capas múltiples y supervisión constante.
- Aplicación: Se implementan firewalls de próxima generación (NGFW), IDS/IPS y filtrado DNS para impedir accesos no autorizados y detectar tráfico sospechoso desde la Internet. Se aplican listas negras, geobloqueo y protección contra ataques DDoS.
- Relación con OSI: Corresponde principalmente a las capas 3 y 4 (Red y Transporte), al controlar el flujo de paquetes.
- Mitigación: Implementar *firewalls de próxima generación (NGFW)* y *filtrado DNS seguro* para bloquear tráfico malicioso y prevenir ataques desde dominios comprometidos.
- Justificación: Esto impide accesos no autorizados y evita que ataques como la explotación de la vulnerabilidad de día cero lleguen a la red interna.

Principios de Defensa en Profundidad

Capa 2: Red Interna / Segmentación

- Principio aplicado: Segmentación de acceso y redundancia.
- Aplicación: Las redes se dividen en zonas lógicas (por función, criticidad o confidencialidad) mediante VLANs y firewalls internos. Esto evita que un atacante pueda moverse libremente dentro de la organización si compromete un sistema.
- Relación con OSI: Aplica a la capa 2 (Enlace de Datos) y capa 3 (Red).
- Mitigación: Aplicar *segmentación de red con VLANs y microsegmentación*, junto con *firewalls internos*.
- Justificación: Limita el movimiento lateral del atacante una vez dentro, conteniendo el compromiso a una zona específica.

Principios de Defensa en Profundidad

Capa 3: Endpoint / Dispositivos

- Principio aplicado: Supervisión constante y menor privilegio.
- Aplicación: En los dispositivos se instalan EDR, control de puertos USB, políticas de actualización automatizadas y antivirus con IA. Se restringen privilegios de administrador.
- Relación con OSI: Incluye desde la capa 1 (Física) hasta la 5 (Sesión), según el tipo de dispositivo
- Mitigación: Instalar soluciones *EDR (Endpoint Detection and Response)* y deshabilitar el uso no autorizado de periféricos (como USB).
- Justificación: Detecta rápidamente actividad sospechosa en los dispositivos y evita la persistencia o ejecución de malware como el recibido por el empleado desde LinkedIn.

Principios de Defensa en Profundidad

Capa 4: Aplicaciones

- Principio aplicado: Capas múltiples y segmentación lógica.
- Aplicación: Uso de WAF, análisis estático/dinámico de código, revisiones manuales y DevSecOps. Las aplicaciones tienen autenticación reforzada y validación de entradas para evitar inyecciones.
- Relación con OSI: Capa 7 (Aplicación), directamente relacionada con la interacción del usuario.
- Mitigación: Desplegar un *Web Application Firewall (WAF)* y actualizar el software obsoleto de gestión de proyectos en la DMZ.
- Justificación: Previene la explotación de vulnerabilidades conocidas y protege contra ataques dirigidos a servicios web.

Principios de Defensa en Profundidad

Capa 5: Datos

- Principio aplicado: Redundancia y menor privilegio.
- Aplicación: Clasificación de información, políticas de retención, cifrado AES-256, sistemas DLP y respaldo automatizado. El acceso a datos está restringido según el rol.
- Relación con OSI: Capas 6 y 7 (Presentación y Aplicación), enfocadas en formato, cifrado y uso de los datos.
- Mitigación: Cifrar bases de datos sensibles en reposo y tránsito, y aplicar soluciones *DLP (Prevención de Pérdida de Datos)*.
- Justificación: Aunque un atacante acceda a los datos, estos no serán legibles; además, se evita su exfiltración no autorizada.

Principios de Defensa en Profundidad

Capa 6: Identidad y Acceso

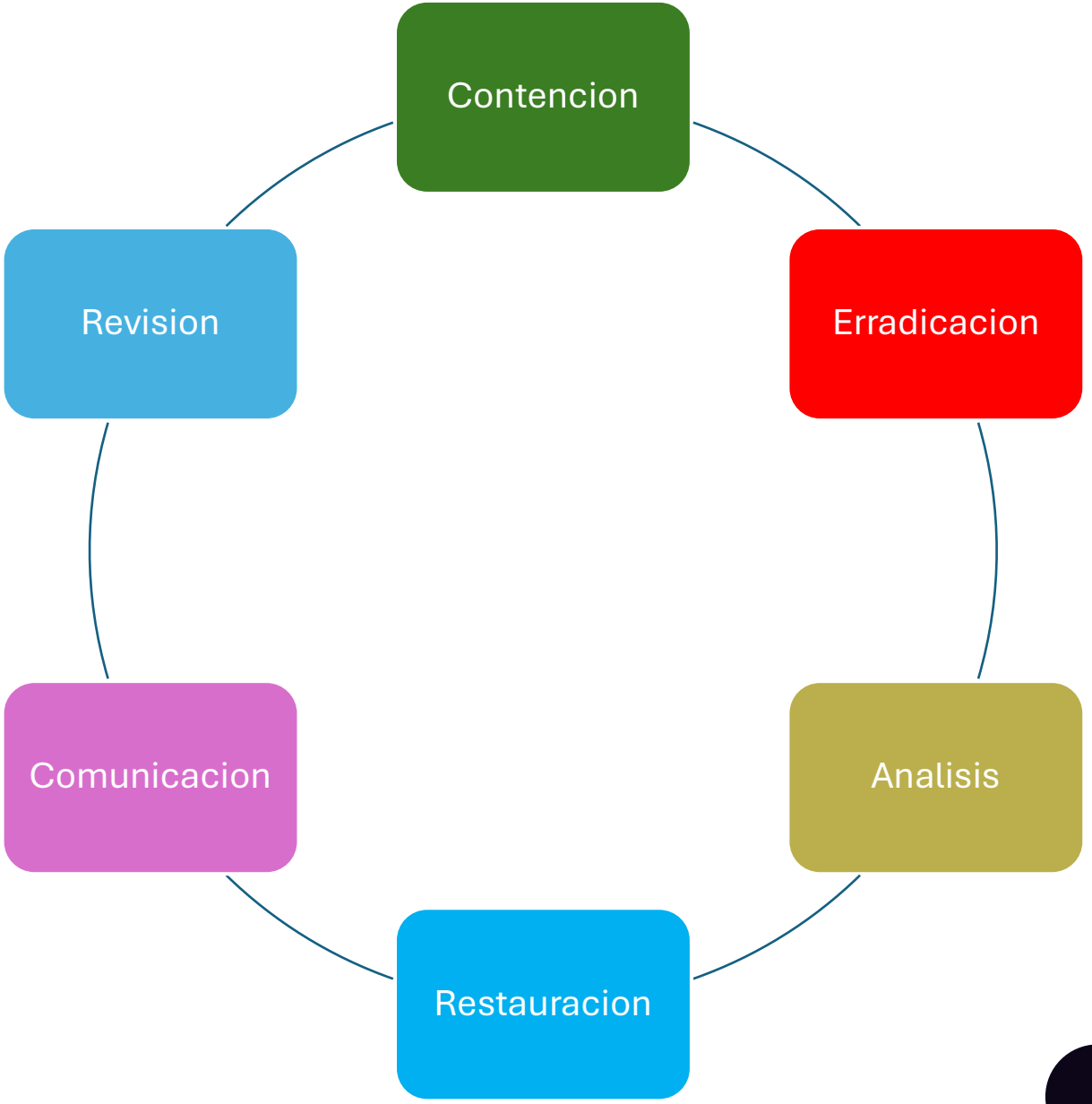
- Principio aplicado: Menor privilegio y redundancia.
- Aplicación: Gestión de identidades con RBAC (Control de Acceso Basado en Roles), autenticación multifactor (MFA), expiración automática de sesiones, monitoreo de accesos y revisión periódica de permisos.
- Relación con OSI: Capas 5 a 7 (Sesión, Presentación y Aplicación), por su vinculación con la validación y gestión de sesiones.
- Mitigación: Activar *autenticación multifactor (MFA)* y aplicar *principios de mínimo privilegio* con auditorías periódicas de cuentas.
- Justificación: Evita que el robo de credenciales permita el acceso a recursos críticos y ayuda a identificar cuentas sospechosas, como las creadas por el atacante.

Principios de Defensa en Profundidad

Capa 7: Operaciones y Concienciación

- Principio aplicado: Supervisión constante y defensa proactiva.
- Aplicación: Capacitación continua al personal, campañas de concienciación, simulacros de phishing, políticas claras y procedimientos documentados. Se mide la cultura de seguridad organizacional.
- Relación con OSI: Transversal, ya que involucra a los usuarios que interactúan con todos los niveles del sistema.
- Mitigación: Ejecutar campañas regulares de *simulacros de phishing* y entrenamientos obligatorios en ciberseguridad.
- Justificación: Reduce la probabilidad de éxito de ataques basados en ingeniería social, como el phishing recibido por los empleados.

Respuesta al incidente



Monitoreo y mejora continua

Implementar un SIEM (Security Information and Event Management) para monitoreo centralizado y correlación de eventos.

Revisar y ajustar las políticas de seguridad según nuevas amenazas y lecciones aprendidas.

Realizar pruebas de penetración y auditorías de seguridad periódicas.

Actualizar y probar regularmente los planes de respuesta a incidentes.

Fomentar la cultura de reporte de incidentes y aprendizaje continuo en toda la organización.

Conclusiones

- **Importancia del enfoque en capas:**

La defensa en profundidad es vital en infraestructuras complejas y reduce el impacto de ataques avanzados.

- **Riesgo por falta de controles:**

El ataque demuestra que sin controles adecuados por capa, un incidente puede escalar rápidamente.

- **Modelo OSI como base estratégica:**

Integrar los controles con el modelo OSI garantiza cobertura técnica completa y coherente.

- **Controles clave y principios esenciales:**

El uso de MFA, segmentación, monitoreo y privilegios mínimos son fundamentales en la prevención.

- **Factor humano como eje de la defensa:**

La formación y conciencia del personal son determinantes para detectar y evitar ataques.

- **Actualización y mejora continua:**

La seguridad debe ser dinámica: auditorías, simulaciones y ajustes periódicos son imprescindibles.

Bibliografía

Instituto Nacional de Estándares y Tecnología. (2018). Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2). https://doi.org/10.6028/NIST.SP.800-61r2

ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks.

Preguntas

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

www.esdegue.edu.co

La ***Escuela Superior de Guerra "General Rafael Reyes Prieto"*** está certificada bajo las normas internacionales **ISO 9001:2015** e **ISO 21001:2018.**

Gracias

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

www.esdegue.edu.co