

JaCkHaCk^{Alert!}

SOFISTICANDO LA VIGILANCIA MES A MES

En el tránsito de las redes, se generan verdaderas “minas de oro” de información técnica, útil para la toma de decisiones operativas y gerenciales de seguridad, y para recopilar incidentes, que son la materia prima de la mejora continua de un SGSI o sistema de gestión de seguridad de la información.

Sin embargo, la extracción de este preciado material está fuera del alcance de las labores corrientes de seguridad, principalmente por el desconocimiento de su utilidad, el tiempo que consume estudiarla y la especialización requerida para procesarla.

Descripción

JaCkHaCk-Alert! es un servicio del monitoreo gestionado de los eventos de seguridad de la red (perimetral o interna)

Características y beneficios

- Reportes ejecutivos mensuales, con gráficas, interpretaciones, incidentes y conclusiones (acumulativos, top ten events, por servicio abierto, por motor, etc)
- Dos consolas de análisis (de tiempo real y de pos-ataque)
- SLA: monitoreo diario, notificación temprana y afinamiento en demanda
- Asesoría trimestral para coordinación y respuesta a incidentes on-site
- NDA bilateral y data bruta alojada en red anfitrión
- Auditoría dual de comandos ejecutados
- Afinamiento por escenario local (positivos falsos, políticas, etc) o global (firmas exploits y vuln.)

Ofrecimiento

JaCkSecurity ha desarrollado JaCkHaCk-Alert!, el servicio de monitoreo de seguridad gestionada. El cometido se logra a través de la implantación de la terminal de monitoreo de seguridad y respuesta a incidentes, *tcp[13]*.

La terminal es –principalmente– un sensor de red monitoreado remotamente vía VPN, equipado con un selecto conjunto de herramientas de análisis y captura, operados con un diseño propietario.

Su ubicación determina el uso o beneficio estratégico seleccionado por la organización.

JaCkSecurity y el uso creativo de los informes

La experiencia de nuestro CTO con este tipo de información le permite aseverar que los reportes del servicio CTO pueden ser empleados para (1) inteligencia de TI, gerencial o legal (2) monitoreo de cumplimiento del soporte TI de terceros (3) conocimiento situacional del perímetro (4) promocionar las políticas de seguridad (5) justificar sólidamente nuevas o pre-existentes inversiones de seguridad (6) hallar o recuperar información forense basada en la red (7) analizar ataques avanzados y (8) la solución de problemas de red.

Aunque no todos los usos son intrínsecos al servicio, los mismos pueden ser ampliados comercialmente según el caso.

Nuestro compromiso

Meticulosidad, correlación, análisis, coordinación y respuesta, actualización, afinamiento y resumen



Nuestros expertos comentan:

“En la actualidad, existen variados *outsourcers* que proveen servicios de seguridad administrada basada en tecnología nueva o pre-existente.

Este tipo de servicios administrados son ofrecidos con el argumento de ahorro en depreciaciones de activos, reducido *head-count*, y respuesta a fallos en 7x24. La idea trabaja bien para organizaciones pequeñas, que no posee personal experto en TI o de seguridad TI.

Sin embargo, opuesto a la creencia, muchos de estos servicios son adquiridos principalmente por grandes organizaciones.

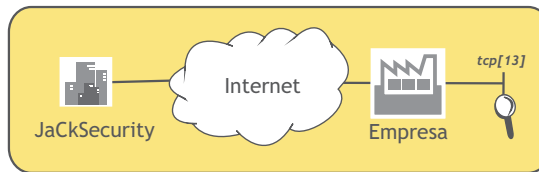
El personal experto de dichas organizaciones queda sorprendido por tan pobre e inexistente análisis de los reportes, por el tiempo de respuesta, y por la nula proactividad del servicio.

Esto sucede porque los servicios de seguridad administrada no están diseñados para organizaciones con altas expectativas, sino para pequeñas organizaciones con necesidades básicas de perimetrización y no de monitoreo”.

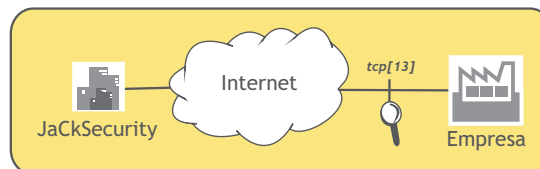
Especificaciones técnicas del servicio

JaCkHaCk-Alert! es fundamentalmente un servicio. El hardware puede ser proporcionado por el cliente. Las especificaciones son:

- Un informe mensual técnico-ejecutivo.
 - Revisión de consola cercana al tiempo real, SLA 45 minutos diarios en 8x5
 - Coordinación de incidentes relevantes o afinamiento de IDS Snort, SLA 3 horas semanales
 - Respuesta a incidentes *on-site* 4 horas mensuales, *on-demand*
- a) JaCkHaCk-Alert! con *tcp[13]* en el perímetro interno, para determinar eventos anómalos generados desde el interior de la red.



- B) JaCkHaCk-Alert! con *tcp[13]* en el perímetro externo.



¿ Por qué JaCkHaCk-Alert! ?

Tiempo real: JaCkHaCk-Alert! posee consolas en tiempo real para gestionar eventos de seguridad de las últimas 24 ó 72 horas durante la semana (8x5). A través de ellas, JaCkSecurity alerta de eventos relevantes, aún antes de la entrega mensual del informe técnico-ejecutivo.

Seguridad administrada: JaCkHaCk-Alert! Imprime reportes avanzados. Ningún tipo de data en bruto es proporcionada al cliente. Todos los reportes son comentados gráfica por gráfica, incidente por incidente y acompañados de conclusiones y recomendaciones.

Outsourcing: JaCkHaCk-Alert! es un servicio de outsourcing diferente. Es posible la intervención del cliente, es decir de operadores especializados con autorización local para realizar análisis en paralelo, a través de acceso a las consolas. Así, los oficiales de seguridad especializados en seguridad y análisis de intrusiones pueden libremente colaborar con los analistas de JaCkSecurity en tiempo real, sin esperar a que un incidente se produzca.