Auditoría de Seguridad de Red NEREA

A lo largo de 2010 se realiza una auditoría de seguridad a la Red NEREA a través de una consultora externa, en el contexto de la Auditoría de Seguridad de la Red Corporativa de la Junta de Andalucía, actividad promovida por el centro de seguridad AndalucíaCERT.

Los resultados de la auditoría son claramente positivos. Se han valorado diferentes aspectos de la red, como la arquitectura, configuraciones, políticas de cortafuegos, etc., habiéndose superado con éxito todas las pruebas. La auditoría se ha estructurado en seis fases, cada una dedicada a un aspecto determinado y concluye cada fase con una valoración general y una serie de recomendaciones.

Las conclusiones de cada fase quedan como sigue:

Fase 1. Revisión de Arquitectura

- Diseño de red: La red está correctamente segmentada. Se destaca además, la redundancia general en todos los nodos, por lo que todos los cortafuegos tienen un alto nigel de recuperación ante posibles fallos hardware.
- Criptografía: Todo el tráfico entre sedes va cifrado, tanto con soluciones “end-to-end” tipo OpenSwan como soluciones “user encryption”, como OpenVPN.
- Alarmas: Se dispone de un sistema Nagios, utilizado para la gestión de alarmas relacionadas con los sistemas de NEREA. Deseable sería un sistema de correlación de eventos de todo lo que se publica vía syslog como eventos de sistema.

Fase 2. Análisis de la política de cortafuegos, conmutadores y routers

- Acceso en puertos altos. Es necesario mantener abiertos puertos altos no convencionales debido a la exigencia de ciertos servicios de terceros que se ofrecen por la red Nerea.
- Patrones de definición de reglas: no se detectan errores en la definición de reglas.

Fase 3. Revisión de configuraciones implantadas en los servicios de red

Se realiza un análisis de alto nivel sobre las configuraciones implantadas en los servicios de la solución (Servidor web Apache, Túneles IPSES OpenSwan, Servidor DNS Bind, Túneles SSL OpenVPN...), localizando los posibles puntos débiles y las recomendaciones en ese mismo nivel para la mejora de la seguridad y fiabilidad estructural de la red. La auditoría otorga una valoración de 7 sobre 10, indicando que la seguridad de las configuraciones es **bastante buena**.

Fase 4. Análisis de vulnerabilidades

Se llevan a cabo desde distintos puntos de la infraestructura de red: CSC, CAR, un AC.

- Pruebas de visibilidad: el filtrado realizado es bueno, ya que se deniega la mayor parte del tráfico no necesario.
- Vulnerabilidades: Se realizan una serie de recomendaciones para mejora, aunque la valoración global es de 9 puntos sobre 10, calificándose la seguridad ante el test de intrusión de **sobresaliente**. La seguridad impuesta es suficiente para impedir que se encuentre ningún factor de riesgo importante:
    - La transmisión de información sensible se realiza de manera segura.
    - Los protocolos inseguros (como telnet) son correctamente bloqueados impidiendo el uso de los mismos.
    - El acceso a los servicios está rigurosamente controlado, permitiéndose sólo los necesarios para el correcto funcionamiento y administración de los mismos.

Fase 5. Análisis de Tráfico

Se realiza un análisis de tráfico a través del sistema de sondas en los diferentes puntos de la red. La conclusión general es que la seguridad de la red es **buena**, ya que el tráfico que transcurre por redes que no están bajo el control de la red NEREA como son Internet o la red MacroLAN por lo general se realizan a través de túneles IPSEC o SSL.

El tráfico que circula por las zonas internas no siempre utiliza los canales o métodos más seguros, aunque el acceso a estas redes en principio es posible únicamente accediendo de forma física a las instalaciones.

Fase 6. Test de Intrusión

Las pruebas han sido realizadas sobre distintos puntos de la infraestructura de la red NEREA:

Centro de Servicios Comunes, Centro de Acceso Remoto, Área de Conexión de Córdoba y la Red Corporativa de la Junta de Andalucía (RCJA).

El esfuerzo realizado para segmentar los distintos tramos de la red, así como el uso de DMZs, y la atención prestada a las reglas de firewall hace que, aunque existan vulnerabilidades, no puedan ser explotadas desde las distintas diputaciones y sean únicamente visibles desde cada DMZ, lo cual reduce en gran medida el impacto de éstas.

La seguridad de los objetivos del alcance del test de intrusión es **notablemente buena**, habiéndose alcanzado la calificación de 8 puntos sobre 10.