Gestión Dinámica de Riesgos: Seguridad de la Red de Servicios

José A. Mañas, Universidad Politécnica de Madrid

Carlos Belso, Centro Criptológico Nacional

Resumen

Actualmente utilizamos sistemas de información como soporte de múltiples servicios a los ciudadanos, tanto dentro del marco de la administración electrónica (ley 11/1997) como en la provisión de servicios industriales (infraestructuras críticas). La seguridad de estos sistemas es crítica y exige tanto un trabajo preventivo como un seguimiento constante de vulnerabilidades e incidentes que permita una gestión adaptada a las circunstancias de cada momento. En esta comunicación se describe cómo analizar dinámicamente los riesgos y tomar medidas adecuadas en una red de sistemas distribuidos que dependen unos de otros sin apenas solución de continuidad.

Palabras clave

análisis de riesgos, gestión de riesgos, seguridad dinámica, seguridad distribuida, esquema nacional de seguridad, ley 11/1997, infraestructuras críticas

1 Introducción

El análisis de riesgos es una actividad clásica que se requiere como base en múltiples ámbitos de la seguridad, desde certificaciones de sistemas de gestión de la seguridad (SGSI, ISO 27001), hasta la protección de los servicios de la administración electrónica (Esquema Nacional de Seguridad, Real Decreto 3/2010).

Clásicamente el análisis de riesgos se ha venido realizando como una actividad de despacho para un análisis preventivo de las medidas de protección adecuadas y proporcionadas al valor de lo protegido frente a una caracterización del entorno hostil en que se encuentra, sea por incidentes externos, ataques deliberados o vulnerabilidades propias del sistema de información.

El análisis estático sólo permite una gestión preventiva. Durante la ocurrencia de incidentes o ataques, es mero observador que aprende de lo ocurrido para el siguiente ciclo de despacho: revisión periódica. Pero no permite un análisis en tiempo real

- cuando descubrimos una vulnerabilidad en nuestro sistema (por ejemplo, un defecto de software o una deficiencia de fabricación o de ensamblaje o de gestión)

- cuando un incidente o un ataque inutiliza parte de nuestras capas de defensa (por ejemplo, desastres naturales o ciberataques); en estos casos el perímetro de seguridad cambia y el riesgo aumenta notablemente
- cuando un proveedor tiene problemas en su prestación de servicio con consecuencias sobre nuestra capacidad de operar

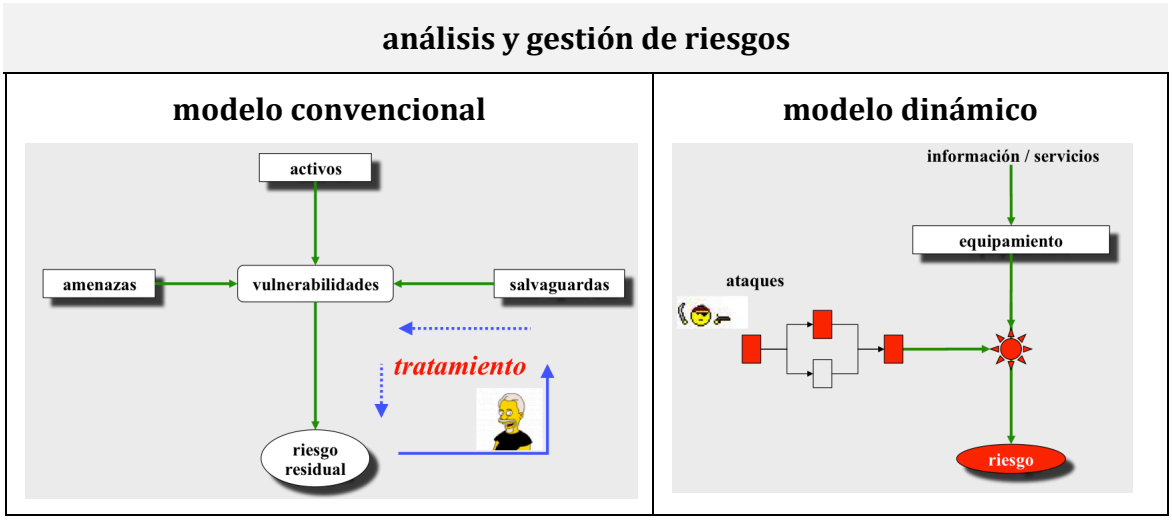
En todos estos casos lo que se requiere es revisar el análisis de riesgos del nuevo escenario y tomar rápidamente decisiones correctivas que mitiguen el impacto y permitan salir lo antes posible del escenario de crisis en que nos hemos visto envueltos.

2 Análisis dinámico de riesgos

Todo análisis necesita un modelo que defina los parámetros de entrada, el procesamiento y el significado de los resultados. En un análisis de riesgos, a veces es tanto o más importante el por qué que el resultado porque si el riesgo es elevado la pregunta relevante es qué debemos hacer para reducirlo y, teniendo en cuenta que el entorno es el que es, normalmente lo que hay mejorar es el sistema de protección propio para que de las mismas premisas se deriven situaciones de mejor riesgo. Eso implica entender cómo se traducen las amenazas en riesgos y cómo frenar las amenazas para que no lleguen a desgracias.

En este modelado pensamos que los incidentes rara vez son atómicos (en el sentido académico del término: indivisibles) sino que usualmente siguen una ruta de avance desde donde se originan hasta donde hacen daño al sistema. Esto es muy gráfico en sistemas que disfrutan de capas de defensa, físicas y lógicas, de forma que un atacante tiene que ir progresando a través de varias etapas, a veces ayudado de forma inconsciente por problemas técnicos que debilitan alguna capa o por catástrofes naturales que destruyen o debilitan el esquema de capas. Un modelo que de respuestas debe incluir este concepto de progreso para poder entender

- qué capas debemos proteger preventivamente para impedir, dificultar o retrasar el progreso del incidente
- qué debemos hacer cuando una capa ha sido perforada y el atacante está más cerca de alcanzar su objetivo: esta es la parte más dinámica, pues supone conectar los detectores de intrusión al sistema de análisis de riesgos para conocer el riesgo sobrevenido tras una intrusión



2.1 Grafos de ataque

A fin de modelar el progreso aprovecharemos el concepto clásico de árboles de ataque para modelas la actividad del incidente o atacante. Con una sutil diferencia. Mientras los árboles de ataque modelan el plan de actuación del atacante (por eso es un árbol de opciones o decisiones), el grafo de ataque modela el progreso del atacante.

Los grafos de ataque son grafos, conjuntos de nodos y arcos, donde los nodos representan etapas en el progreso del atacante hacia el objetivo. Esta orientación hacia el objetivo hace que los grafos sean unidireccionales o acíclicos. Al igual que los árboles, hay diferentes formas de llegar a un cierto punto intermedio, bien formas alternativas (OR) o formas de llegar que requieren la conjunción de éxitos (AND). Y, a diferencia de los árboles de ataque, hay ramificaciones tras una etapa

- para modelar que hay varias opciones para seguir tras un éxito parcial (por ejemplo, seguir rompiendo barreras físicas o pasar a ciberataques lógicos
- para modelar que hay varios finales posibles del ataque: daño a más de un activo o en más de una dimensión (por ejemplo robando cierta información, manipulando las trazas de actividad e interrumpiendo un servicio)

2.2 Adaptación de Magerit

Magerit es la metodología de análisis y riesgos recomendada en la administración pública española. El modelo de cálculo riesgo de magerit tiene en cuenta el impacto y la probabilidad de que tenga lugar para derivar la estimación de riesgo.

En un escenario de incidentes por etapas, el impacto puede no ser único sino incremental, poco a poco, por lo que necesitamos una función de acumulación de impactos parciales. Para ello se utiliza la misma formulación matemática que para calcular grados de dependencia y riesgos repercutidos (en terminología de Magerit).

Igualmente, en un escenario de incidentes por etapas, la probabilidad de que el incidente culmine con 'éxito' una etapa depende de su posición en el grafo. Cuando las etapas previas han sido superadas, una etapa se encuentra expuesta a la pericia del atacante. De esta forma tenemos probabilidades condicionales, en donde la probabilidad de una etapa está condicionada por la probabilidad de las anteriores.

Siempre hay una probabilidad base para el caso de que las etapas anteriores estén consumidas (por ejemplo, cuando los sistemas de detección de intrusión informan del éxito de una penetración: ya no hay etapas previas que superar, el enemigo está en la puerta).

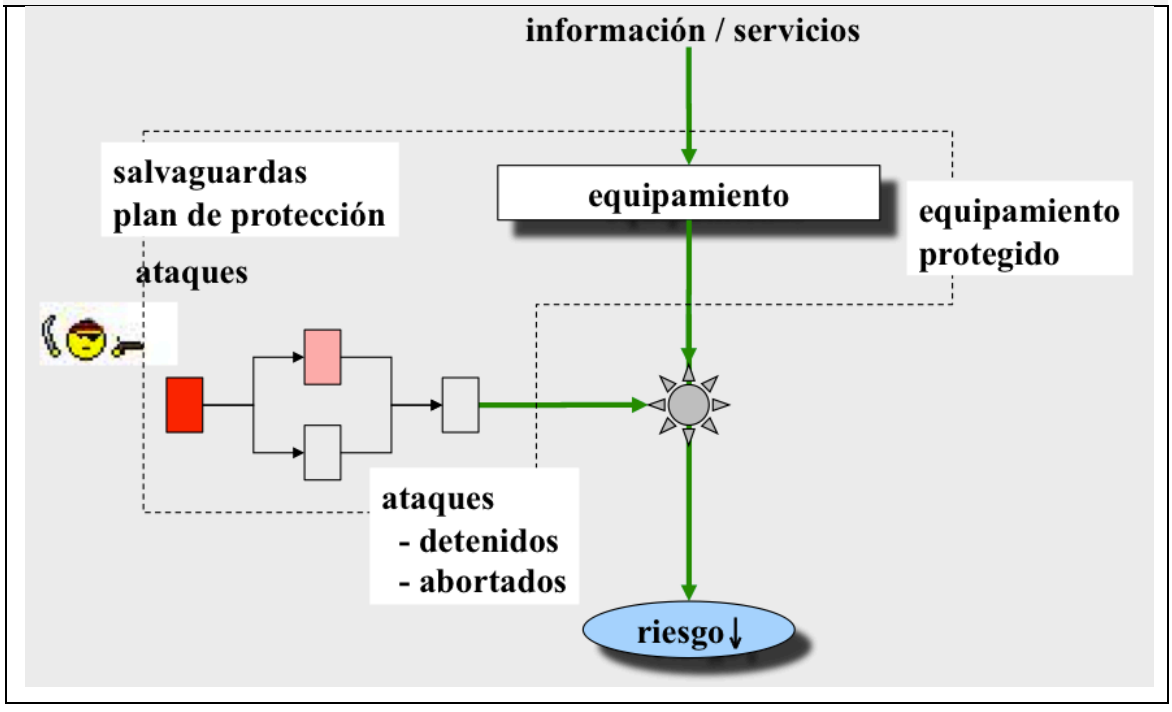
El conjunto de grafos, impactos acumulados y probabilidades condicionales nos permite

- modelar una defensa preventiva basada en capas de defensa
- incorporar dinámicamente situaciones sobrevenidas donde el esquema de capas ha sido violentado
- analizar el riesgo 'en reposo' y durante una situación de crisis

3 Gestión dinámica de riesgos

Una vez disponemos de un modelo que se adapta a las circunstancias para realizar un diagnóstico del riesgo en tiempo real, lo siguiente es reaccionar en tiempo real a las circunstancias. Evidentemente, el análisis es una herramienta esencial para tomar decisiones informadas.

tratamiento dinámico de riesgos



Ahora entra el juego el factor tiempo, pues para evitar que un incidente se transforme en una desgracia lo que hay que hacer es reaccionar con rapidez. Simplemente basta ser más rápidos en la reacción que el incidente o el atacante en su progreso.

En términos matemáticos, el modelo de magerit adaptado en la sección anterior al análisis de grafos lo enriquecemos un poco más con el concepto de 'ventana de tiempo' o ventana de oportunidad. Es simplemente una corrección proporcional de la probabilidad condicional de que una etapa se consume. Cuando un atacante

supera una etapa, abre una ventana de tiempo durante la cual puede intentar el siguiente paso. Esta ventana de tiempo la cierra el sistema de defensa. Basta incorporar el tiempo de reacción al modelo para poder recortar en proporción la ventana de ataque.

Un sistema completo de gestión de crisis tienen en cuenta también que la capacidad de defensa es dinámica. Es clásico el uso de maniobras de distracción que consumen recursos para la defensa atacando por varios puntos simultáneamente. La capacidad de respuesta se ve mermada por los recursos ya consumidos. Todo esto vuelve a entrar en el sistema de análisis para un diagnóstico preciso y ajustado a las circunstancias cambiantes.

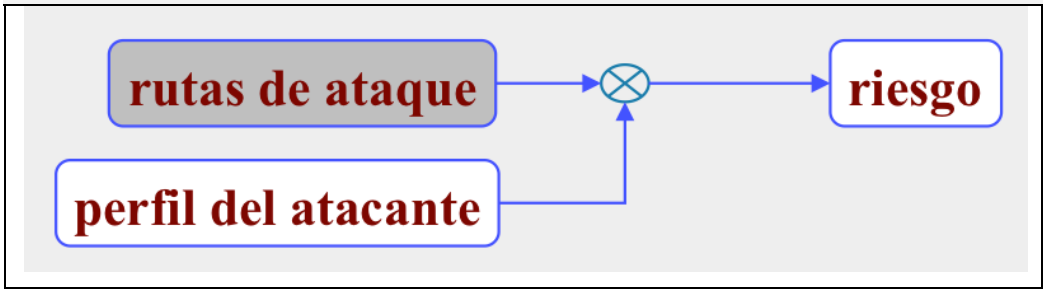
3.1 Perfil del atacante

Por otra parte hay que entender quién ataca. No todos los atacantes son iguales. Varían sus habilidades, su capacidad económica, su velocidad de actuación e incluso su acceso al perímetro del sistema.

El análisis de sus habilidades nos lleva a ajustar las probabilidades de que el atacante logre superar una etapa en más o menos tiempo. Este concepto se viene utilizando en la certificación de productos bajo el nombre de "potencial del atacante" y permite emitir certificaciones de productos que evalúan la resistencia del objeto certificado frente a una cierta categoría de atacantes. No es lo mismo un aficionado ocasional que un profesional, o un equipo atacante especializado en una oscura vulnerabilidad del producto.

Por otra parte, el conocimiento de la posición del atacante nos permite situarlo en una etapa inicial del grafo de ataque. No es lo mismo un atacante externo que tiene que atravesar todas las barreras defensivas, que un atacante interno que empieza a actuar más cerca del objetivo final.

cálculo del riesgo como combinación de grafos y habilidades del atacante



4 Sistemas distribuidos

Ya no hay sistemas aislados. Todo se está conectado. Las debilidades de mis proveedores son el origen de mis riesgos.

Dicen que el mundo es una pequeña aldea de alcance global, y aparece la tentación de hacer un modelo matemático de dicha villa. Modelo que, simplemente, es irrealizable porque

- es demasiado complejo

- choca con la fragmentación de dominios de seguridad: no hay un responsable de la aldea global, hay muchos, con prioridades propias y no necesariamente convergentes; hay sector privado y sector público, hay intereses políticos e intereses comerciales, a corto y a largo plazo, y hay estados soberanos que aceptarán colaborar … o no
- choca con secretos, sean industriales, operacionales o de estados soberanos, lo que obliga a trabajar con las interfaces (servicios prestados y recibidos) sin conocer las entrañas
- choca con la necesaria especialización de cada sistema: no es lo mismo un entorno industrial que una operadora de comunicaciones o el sistema sanitario; cada uno necesita modelos propios de análisis y gestión de riesgos

Esta fragmentación nos lleva inmediatamente a la necesitar de analizar y gestionar un sistema distribuido en el que

- debemos vocear el conocimiento de las vulnerabilidades sobrevenidas (esto lo vienen haciendo redes sectoriales como los CERT en el entorno de sistemas de información)
- debemos vocear el conocimiento del atacante (hay muchas variantes, desde ataques industriales hasta terrorismo, donde aparece la comunidad de inteligencia con capacidad para conocer con un amplio alcance)
- debemos establecer una conexión de los análisis (dinámicos) de los sistemas interconectados; esto es, el reporte del nivel de riesgo de los servicios prestados, que se propaga a los que prestan servicios de valor añadido

Dicen que infraestructuras críticas son las que sustancian la prestación de servicios críticos. Pues bien, siendo los servicios lo que hay que proteger, las infraestructuras que los prestan pueden ser críticas en sí mismas (porque son punto único de fallo) o críticas en ciertas circunstancias (porque se han quedado solas o porque sus capas de defensa están seriamente comprometidas). El responsable de una infraestructura crítica tiene que proteger lo mejor posible su responsabilidad; pero el coordinador general tiene que hacer que suene bien el concierto, aunque falle un violín y esté enfermo el tenor titular.

Para alcanzar esta capacidad de análisis y gestión global necesitamos un lenguaje común que podamos usar para entendernos:

- una codificación de activos: servicios, equipamiento e infraestructuras industriales y humanas
- una codificación de la caracterización de atacantes y vulnerabilidades
- una codificación de la estimación de riesgo

5 Herramientas

El Centro Criptológico ha venido apoyando el desarrollo de la herramienta Pilar de análisis y gestión de riesgos, herramienta que tiene dos facetas, la de poder realizar análisis en sistemas reales, y la faceta de servir de banco de experimentación de nuevas ideas como las presentadas en esta comunicación. Esto nos permite saber que lo aquí expuesto funciona, aunque la explotación en sistemas reales constituye un serio reto de integración. En escenarios de

despliegue real, entendemos que Pilar trabajará como un motor de análisis de riesgos al que hay que alimentar con el conocimiento de las rutas de ataque y la caracterización del atacante, amén de ser necesaria una capa de presentación de los resultados para la toma eficaz de decisiones en la cadena de autoridad. Estos son los retos que vamos a acometer en el futuro próximo.

6 Conclusiones

Estamos trabajando para disponer de modelos matemáticos y herramientas prácticas que soporten las necesidades indicadas: análisis de riesgos que sean capaces de entender los ataques que se están produciendo e informar adecuadamente a los que tienen que tomar decisiones preventivas y reactivas de forma que protejamos, no los componentes, sino los servicios finales, sean relativos a la administración electrónica o a los servicios públicos esenciales que a fin de cuentas, están fuertemente interrelacionados.

7 Agradecimientos

El trabajo presentado se realiza en colaboración con

- el proyecto "SEGUR@ - Seguridad y Confianza en la Sociedad de la Información" liderado por Telefónica Investigación y Desarrollo dentro del Programa CENIT del Ministerio de Industria,
- el proyecto "eCID – *Enlightened Critical Infrastructures Protection*" liderado por Indra dentro del Plan Avanza I+D del Ministerio de Industria y Turismo
- el CNPIC (Centro Nacional para la Protección de Infraestructuras Críticas) del Ministerio del Interior.