SERVICIOS DE SEGURIDAD PROACTIVA

Planteamiento de un Sistema de Seguridad Proactivo Global

Área de Seguridad de Mnemo S.A.

¡

1. INTRODUCCIÓN

La palabra “seguridad” aparece en 27 ocasiones en el texto de la LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Algunos de los puntos que argumentan los Servicios de Seguridad que se plantean son:

EXPOSICIÓN DE MOTIVOS

> Depende de la confianza y seguridad que genere en los ciudadanos y depende también de los servicios que ofrezca.

Artículo 3. Finalidades de la Ley.

> 3. Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

Artículo 6. Derechos de los ciudadanos.

> i) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Artículo 9. Transmisiones de datos entre Administraciones Públicas.

> 1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

Artículo 42. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

> 2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

2. ANTECEDENTES

En un entorno reducido, la seguridad informática puede solucionarse a través de mecanismos sencillos como con un sistema de aislamiento local. Sin embargo, una entidad que se expande por una amplia área geográfica y que dispone de servicios electrónicos a terceros debe considerar además problemas derivados de establecer una red de comunicaciones ancha, que implica medidas de seguridad que nos permitan proteger la integridad y la confidencialidad de la información circulante, así como la seguridad lógica del sistema.

Por ello, es importante conocer cómo establecer directrices generales y distribuirlas, así como métodos de verificación de su cumplimiento. Además, debe de considerar no sólo la protección de los sistemas, sino también de toda la infraestructura de comunicaciones y las diferentes tecnologías en las que transita la información.

En este sentido, se hace imperante conocer la estructura de las redes de comunicaciones para, de esta manera, poder sentar las bases de implantación de medidas de seguridad para proteger la información en tránsito por dichas fuentes de información.

Por otro lado, Internet es un medio heterogéneo en el que circulan ingentes cantidades de información. En ocasiones, la inexperiencia de los usuarios pone en riesgo los sistemas y servicios de las Administraciones o Empresas con las que tienen algún tipo de vinculación. Véase por ejemplo el acceso a usuarios y contraseñas a partir de información descargada desde clientes P2P facilitada por usuarios que han configurado incorrectamente el mismo. De igual modo, Internet es un gran foro de reunión en el que se organizan, en algunos casos, ataques distribuidos contra objetivos concretos que pueden ser previstos si son identificados.

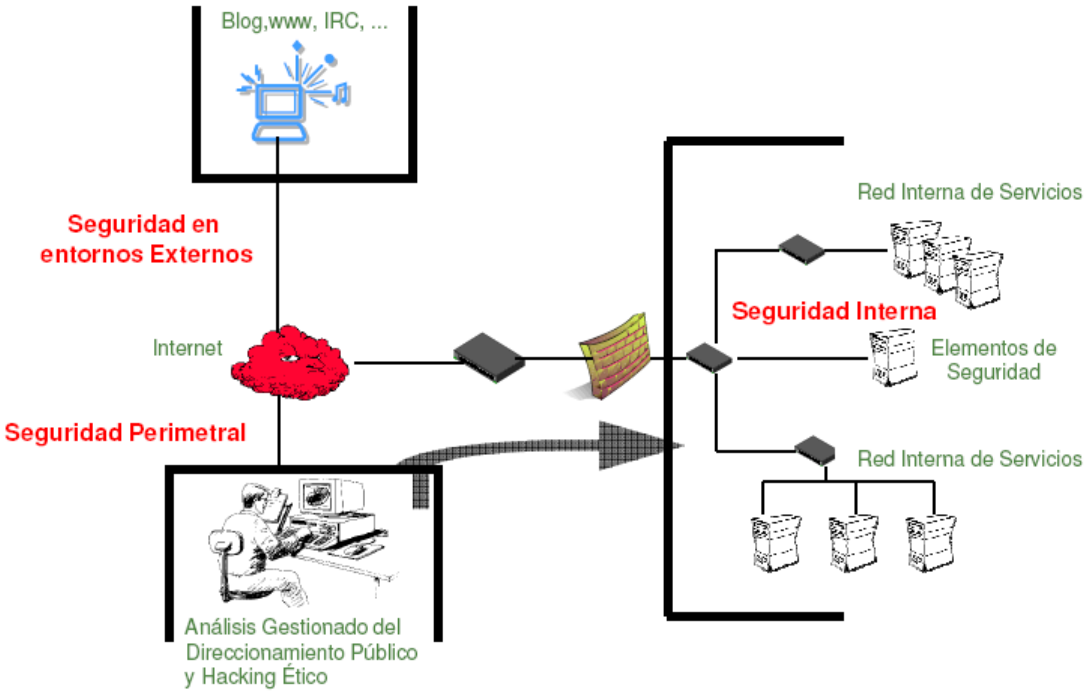
Pero, ¿cómo parecía el ciudadano la seguridad?

3. SITUACIÓN ACTUAL

La Ley para el Acceso Electrónico de los Ciudadanos a los Servicios Públicos reconoce a los ciudadanos su derecho a relacionarse electrónicamente con las administraciones públicas, así como la obligación de éstas a garantizar ese derecho.

El acceso electrónico a los servicios públicos implica una serie de riesgos derivados de amenazas relacionadas con las tecnologías que subyacen tras los mismos. El activo más importante a proteger en este caso es la información de los ciudadanos y para ello no es suficiente el típico planteamiento basado en firewalls, IPS y demás dispositivos de seguridad, que en ningún caso debe de ser descuidado.

Dado que el objetivo es transmitir seguridad al ciudadano, el planteamiento de gestión de la seguridad debe de ser proactivo y global. Para ello, los entornos y tecnologías que deben de ser monitorizados son los que aparecen en el siguiente gráfico:



4. SEGURIDAD EN ENTORNOS EXTERNOS

Objetivos

Los objetivos del Servicio de Seguridad en entornos Externos se basan en la prevención activa sobre las siguientes amenazas:

- Alerta temprana contra “ciberocupas”
- Phishing
- Identificación de amenazas en chats, foros, etc a las distintas Administraciones
- Vigilancia de los posicionamientos y asociaciones de logos y productos de la Administración en websites externos y canales indirectos
- Protección de Datos Personales

Existen otras amenazas en la actualidad y día a día surgen nuevas vulnerabilidades que deben de ser tenidas en cuenta.

Percepción del Servicio

La percepción del Servicio de Seguridad en entornos Externos viene dada por la identificación de los siguientes eventos:

- Análisis sobre dominios. Verificación de dominios en Internet y permutaciones de palabras que son nombres o acrónimos de las Administraciones públicas en los dominios de Internet
- Análisis de contenido no deseado en Internet. Basado en el reconocimiento de imágenes y logotipos.
- Información relevante sobre personas que pueda aparecer en sitios ajenos a su conocimiento.
- Prevención y análisis sobre sitios que cometan o puedan cometer acciones de fraude sobre servicios de las Administraciones Públicas

Integración de información

Ciclo de gestión de la información pasa por extraer la información de todas las fuentes disponibles en Internet, organizarla y correlacionarla con el fin de identificar los eventos de seguridad relevantes e incluso relacionar incidentes detectados en fuentes de información distintas.

Por ejemplo, el hallazgo de un fichero que contenga información para el acceso a un sistema de información específico en el que aparezcan datos personales de un usuario y la identificación de alguno de los datos personales en un foro del mismo en un foro o chat establece una relación entre los mismos.

5. SEGURIDAD PERIMETRAL

Objetivos

Los objetivos del Servicio de Seguridad Perimetral (que nada tiene que ver con la gestión de firewalls, IPS, etc) se basan en la prevención activa en base a las siguientes prácticas:

- Mejora continua de la seguridad de los entornos Internet realizando un seguimiento evolutivo mediante el uso de Normas Estandarizadas y Control Continuo
- Identificación de vulnerabilidades en los activos públicos que se encuentran en la red perimetral a través de acciones de "hacking ético"
- Señalar la manera de corregir las vulnerabilidades encontradas, incluido mecanismos de aviso urgente para las vulnerabilidades más graves.
- Establecer un canal de alertas de vulnerabilidades de seguridad potenciales en la Administración Pública, así como proveer de un soporte especializado como ayuda para la resolución de los problemas de seguridad encontrados
- Diseminar en la Administración Pública el conocimiento de las "mejores prácticas" para la fortificación de los sistemas de la información, así como facilitar la disponibilidad de estándares de seguridad para su aplicación en las tecnologías hardware/software de más amplia difusión en la compañía

Percepción del Servicio

La percepción del Servicio de Seguridad Perimetral viene dada por la información generada desde el mismo:

- Informes de seguridad gestionada sobre las direcciones IP en Internet de la Administración, señalando la manera de corregir las vulnerabilidades encontradas
- Informes de seguridad manual sobre direcciones IP del rango público
- Establecimiento de un mecanismo de aviso urgente para las vulnerabilidades detectadas más graves (Alertas Urgentes)
- Establecimiento de un canal de comunicación, en el que los responsable de seguridad puedan acceder a la información y conocimiento interno de seguridad del que se dispone
- Diferentes Informes de Seguridad dirigidos hacia cada Administración tratando de identificar posibles puntos débiles en la seguridad

Ámbito de los análisis

El análisis de seguridad no se debe de limitar a los entornos de redes convencionales ya que existen innumerables amenazas en otros ámbitos como:

- Análisis de seguridad IP sobre Wifi
- Análisis de seguridad IP sobre UMTS
- Análisis de seguridad IP sobre 3G

6. SEGURIDAD INTERNA

Objetivos

Los objetivos del Servicio de Seguridad Interna se basa en la identificación de eventos de seguridad:

- Identificando las amenazas al negocio
- Integrando la plataforma de monitorización y correlación con los sistemas internos
- Definiendo los eventos de seguridad a identificar
- Normalizando los eventos de seguridad
- Desplegando sondas y plataformas para la identificación de eventos de seguridad
- Monitorizando de forma individual por cada Administración sus eventos de seguridad
- Monitorizando de forma global la correlación de eventos de seguridad en las Administraciones Públicas con el objetivo de dar más valor a la información individual y agrupando eventos de seguridad a nivel superior.

Percepción del Servicio

La percepción del Servicio de Seguridad Interna viene dada por:

- Incremento en la eficacia de la gestión y monitorización de eventos de seguridad.
- Correlación de eventos de seguridad a nivel del conjunto de Administraciones.
- No invalida el esfuerzo e inversión realizados por las Administraciones que ya dispongan de sistemas de correlación de eventos.
- Las soluciones planteadas deben ser multiplataforma y la arquitectura tecnológica que las soporta permitirá la correlación de eventos individuales antes de ser transformados en eventos de seguridad.
- Permite detectar y relacionar eventos de seguridad que afecten a diferentes Administraciones, para que su defensa pueda ser coordinada.
- Permite la definición de diferentes umbrales adaptables a cada Administración.

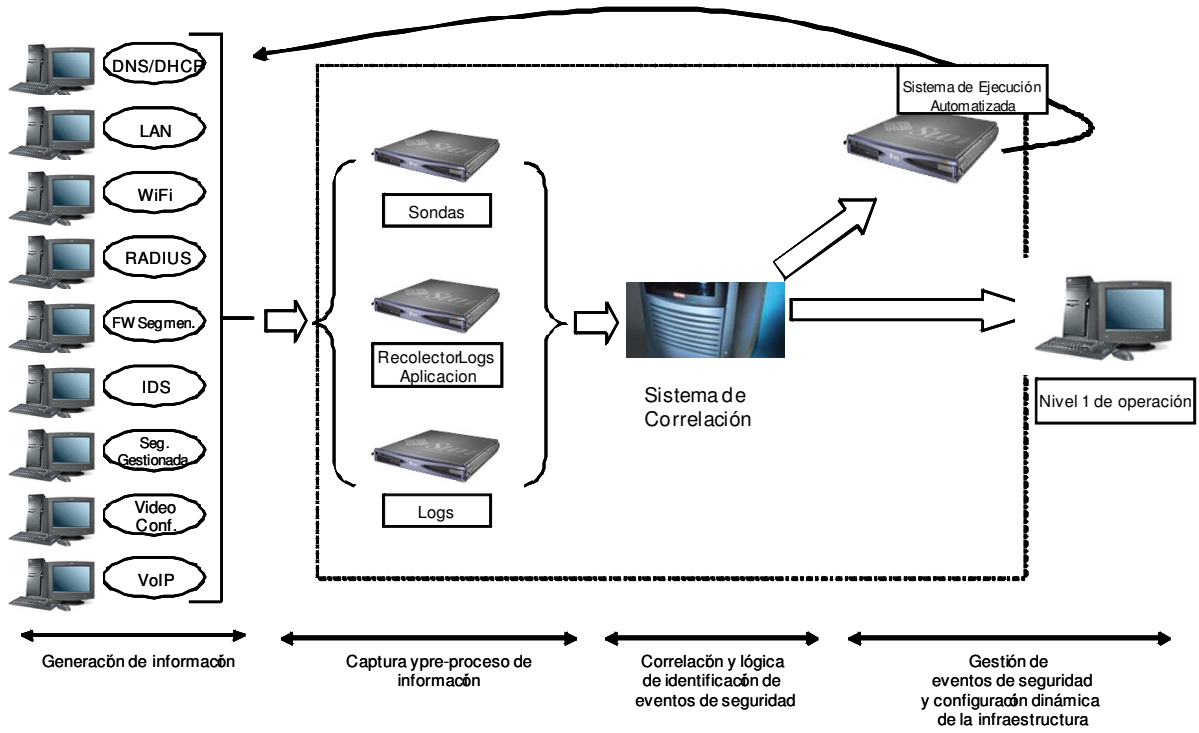
Funcionalidad

La Seguridad Interna permite, como monitor centralizado de eventos de seguridad:

- Identificar y procesar eventos de seguridad producidos en servicios o componentes de red a causa de intrusiones, virus, código malicioso u otras acciones que puedan comprometer la seguridad de las infraestructuras disponibles
- Soportar la integración y correlación de eventos distribuidos entre diferentes servidores, dispositivos y aplicaciones
- Ejecutar acciones que permitan cortar el tráfico en origen, de los puntos de red que se identifiquen como amenazas
- Soportado y desarrollado por un equipo dedicado
- Basado en los Estándares de Seguridad Internacionales

Arquitectura de la solución

La implantación del servicio consiste en el despliegue de diferentes sondas automatizadas que adquieren la información y la transfieren hacia un recolector central.



A partir de la correlación de la información obtenida se emitirán las alarmas correspondientes y se cortará, siempre que sea factible, el tráfico que suponga una amenaza de seguridad.

7.- COLABORACIÓN ENTRE LOS SERVICIOS DE SEGURIDAD

La integración de los diferentes Servicios de Seguridad planteados permite una mejor identificación de los riesgos en el global de los ámbitos en los que fluye la información.