Sistema de Alerta Temprana de Sondas de Internet del CCN-CERT

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

Los incidentes de seguridad a los que están expuestos los sistemas de la Administración Pública española son cada día más numerosos y, a través de Internet, más fáciles de llevarse a cabo y de propagarse. Código dañino y/o espía instalado en los equipos de un Organismo, gusanos que intentan extenderse por la red y comunicarse con servidores externos para enviar información o para destruir o modificar datos almacenados, ataques contra los servicios web de un ente público… En general, este tipo de ataques y especialmente los de código dañino han experimentado un crecimiento exponencial en los últimos años, superando muchas veces a las capacidades de detección tradicionales.

El disponer de una visión holística y distribuida de los riesgos y amenazas que se producen en los distintos organismos, frente a una visión centrada en el tráfico de una única organización, permite mejorar de una forma muy importante las capacidades de detección de tráficos "anómalos" que, de otro modo, podrían pasar desapercibidos.

Esta visión global permite, no sólo detectar incidentes de forma temprana generando las contramedidas más adecuadas para atajar su impacto de la forma más rápida posible, sino que además impide la propagación del incidente a otros organismos y/o dominios.

Ya no basta con responder y gestionar el incidente una vez se ha producido, sino que es necesaria una labor proactiva que permita actuar antes de que el ataque haya penetrado en los sistemas o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance para evitar su propagación a través de la red. De forma análoga, uno de los puntos más importantes para la detección temprana de un posible código dañino que haya infectado sistemas de la organización, es la capacidad de disponer de una visión global.

Por este motivo, desde el año 2008 el Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) viene desarrollando un Sistema de Alerta Temprana (SAT) para la detección rápida de incidentes y anomalías dentro del ámbito de la Administración que permite realizar acciones preventivas, correctivas y de contención. En un primer momento, este servicio comenzó su desarrollo con la monitorización de la Red de Intercomunicación de todos los organismos de la Administración Pública española, SARA. Posteriormente, ya en el año 2009, el servicio se extendió a los accesos de Internet de las distintas administraciones (SAT de Internet).

A través de este servicio, el Centro Criptológico Nacional, en colaboración con el organismo adscrito, puede detectar todo tipo de ataques, evitando su expansión, respondiendo de forma rápida ante el incidente detectado y, de forma general, generar normas de actuación que eviten futuros incidentes. Al tiempo, y gracias al almacenamiento de un número progresivo de eventos, es posible contar con una panorámica completa y veraz de la situación de los sistemas de las administraciones públicas españolas que posibilite una acción preventiva frente a las amenazas que sobre ellas se ciernen.

2. ¿QUÉ ES EL SISTEMA DE ALERTA TEMPRANA DE INTERNET?

El Sistema de Alerta Temprana (SAT) de Internet es un servicio desarrollado e implantado por el Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna del Organismo adscrito e Internet. Su misión es detectar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos. En ningún momento se centra en el análisis del contenido del tráfico, que no sea relevante en la detección de una amenaza.

Para su puesta en marcha es necesaria la implantación de una **sonda individual** en la red pública del Organismo, que se encarga de recolectar la información de seguridad relevante que detecta y, después de un primer filtrado, enviar los eventos de seguridad hacia el **sistema central** que realiza una correlación entre los distintos elementos y entre los distintos dominios (organismos). Inmediatamente después, el Organismo adscrito recibe los correspondientes avisos y alertas sobre los incidentes detectados.

La sonda es un servidor de alto rendimiento y dedicado, que incorpora varias herramientas de detección y monitorización opensource y comerciales (NIDS, arpwatch, ntop, etc..) y que cuenta con dos interfaces de red diferenciados:

- Interfaz de análisis: recibe todo el tráfico a analizar. Este interfaz sólo lee el tráfico, sin modificarlo en ningún momento, y sólo aquel que es necesario para su función (no datos que puedan considerarse sensibles –payload-).
- Interfaz de gestión: conecta a través de Internet de forma segura con el sistema central de monitorización/correlación, haciendo uso de la infraestructura del Organismo o de una conexión independiente.

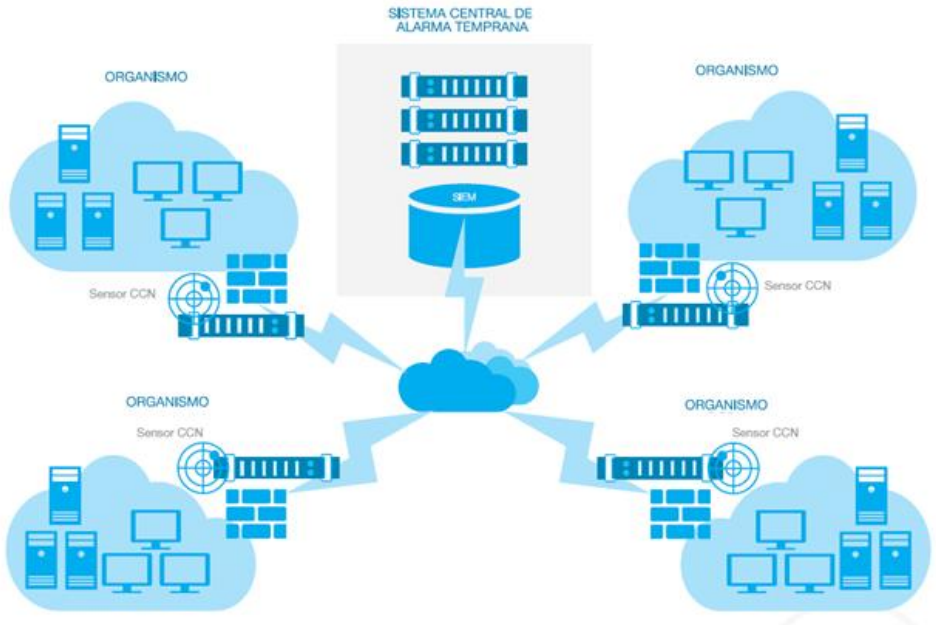

Figura 1. Arquitectura Sistema de Sondas de Internet

El despliegue de la sonda se realiza del siguiente modo:

- Se **estudia** junto al Organismo la **arquitectura de red actual**, y se elige la mejor forma de integración en la red de forma que cause el menor impacto.
- La conexión entre la sonda y el sistema central se realiza siempre de forma **segura**, a través del establecimiento de un túnel OpenVPN. Esta conexión puede realizarse de forma directa (a través de una salida dedicada hacia Internet, ej. adsl) o indirecta (a través de los firewalls del Organismo adscrito). El establecimiento de este túnel cifrado se inicia desde la sonda hacia el sistema central, no siendo necesaria ninguna infraestructura adicional por parte del organismo para el establecimiento de túneles cifrados.
- La sonda se **gestiona** completamente desde el CCN-CERT, no siendo necesaria la realización de tareas de administración por parte del personal del Organismo. Eventualmente se solicitaría apoyo al Organismo en el caso que fuera necesaria la realización de tareas puntuales que no pudieran realizarse de manera remota.
- De forma general, salvo que se pacte otra cosa, la sonda vigilará el **tráfico de salida** a Internet, o de alguna de las DMZ's que se decidan, no entrando en el tráfico interno del Organismo. Con los eventos recibidos se realiza una correlación avanzada de eventos en el sistema central, permitiendo la detección de ataques distribuidos hacia los distintos organismos adscritos al sistema.
- La **gestión, actualización y mantenimiento** del **sistema central** está a cargo del CCN-CERT, que lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de nuevas funcionalidades y herramientas. De hecho, periódicamente se realiza la integración de numerosas reglas de detección, propias y externas, completando y ampliando la inteligencia del servicio y su capacidad de detección. Las reglas propias son generadas a partir de la inteligencia que se produce en el análisis "multidominio" (realmente efectivas para ataques "0 day"), a partir de la información obtenida durante la investigación de otros incidentes de seguridad y a partir de la información recibida de otros organismos con los que se mantiene un intercambio de información referente a incidentes de seguridad. Asimismo, el sistema incorpora adicionalmente otros mecanismos de detección no basados en firmas, como los basados en anomalías de paquetes, flujos de aplicaciones o en el análisis de información de tráfico.
- Los usuarios pueden acceder en tiempo real a **información relevante** de los eventos recibidos, a través de la consola de explotación o a través de los informes restringidos, donde cada Organismo puede ver exclusivamente los eventos e informes relacionados con su red monitorizada.

3. BENEFICIOS APORTADOS A LOS ORGANISMOS ADSCRITOS

El Sistema de Alerta Temprana de Internet tiene como principal función la **protección proactiva** (aplicación de medidas antes de que se produzca un incidente o sea detectado) y **protección reactiva** (en el caso de producirse un incidente, la rápida detección del sistema permite la aplicación de medidas de contención y eliminación de la amenaza necesaria para evitar el incidente). Ofrece **ventajas significativas con independencia de que se tenga una solución de monitorización desplegada** (siendo compatible con ella) o no. En este último caso, permite desplegar una solución gestionada por un equipo de expertos y que incorpora las últimas tecnologías.

En el caso de tener una solución ya implantada, el Sistema de Alerta Temprana de Internet puede ser un complemento perfecto de cualquier solución de monitorización/IDS ya instalada, aportando:

- Incorporación continua de nuevas funcionalidades y herramientas al sistema.
- Integración periódica de reglas de detección (tanto propias como externas).
- Análisis de anomalías en los paquetes o flujos de las aplicaciones.
- Visión holística y agregada de multitud de sondas y organismos, con independencia del proveedor, su tecnología y sus actualizaciones.

El CCN-CERT, además, facilita una distribución personalizada de sus herramientas con los componentes, configuraciones y bastionados seguros y necesarios para su correcta explotación.

En general, las ventajas para cualquier organización podrían resumirse en las siguientes:

- **Detección** de todo tipo de ataques e incidentes, incluyendo **detección avanzada interdominio** (detección temprana de un incidente que se haya replicado en otro de los dominios monitorizados).
- **Correlación**. El sistema central no solo detecta incidentes importantes de forma individual, sino que se pueden detectar eventos mucho más complejos que pueden involucrar a distintos dominios. Al tratarse desde una perspectiva global, cotejando y comparando los diferentes incidentes recibidos por cada sonda, se está en disposición de realizar una mayor y mejor identificación de los incidentes.
- Acceso al mayor conjunto de **reglas de detección**, tanto propias como externas, integradas por el equipo de expertos del CCN-CERT que permite la detección de un mayor número de amenazas.
- **Información** de gran valor para los responsables TIC de las administraciones públicas, que pueden ver en tiempo real el estado de su red con respecto a la seguridad, así como acceder a informes estadísticos.
- **Soporte a la resolución de incidentes**. Como CERT Gubernamental español, el CCN-CERT ofrece a todos los organismos su colaboración para una detección, contención y eliminación de cualquier ataque que pueda sufrir a sus sistemas.

4. PREGUNTAS MÁS FRECUENTES - FAQ -

4.1 ¿Qué es una sonda?

La sonda es un servidor de alto rendimiento que permite la recolección de información de la red especificada por el Organismo adscrito, el filtrado de los eventos específicos de seguridad y su envío de forma segura al sistema central. Consta de los siguientes elementos:

- El interfaz de gestión, que se conecta a la red del Organismo para enrutar el tráfico hacia Internet (siempre consensuado con el Organismo que se adscribe).
- Los interfaces de análisis, que no tienen IP y son totalmente transparentes a la red.
- Un Sistema de Detección de Intrusiones de Red Snort (IDS), con reglas de detección específicas de diferentes fuentes y creación propia.
- Un agente de la herramienta SIEM OSSIM, que permite la depuración de los eventos detectados y su envío al Sistema Central. Este agente inicialmente está configurado para el análisis de los eventos generados por las distintas herramientas de detección que incorpora (Snort, ARP Watch, p0f, etc.).

4.2 ¿Dónde se instala la sonda?

La sonda puede implantarse en distintos puntos de la red dentro de la infraestructura del Organismo, pero siempre en un punto en el que únicamente se visualice tráfico con direccionamiento público del Organismo.

Además, esta sonda puede estar conectada a distintas redes para realizar una monitorización diferenciada, siempre que existan diversas interfaces de red disponibles para esta tarea.

En cada caso se estudiará junto con el Organismo cual es la situación ideal donde realizar la instalación de la sonda. Esta decisión se tomará en consenso con el Organismo, ya que mientras la instalación de la sonda dentro del primer perímetro de seguridad, justo después del firewall externo de la organización, permite tener una visión más clara de los posibles incidentes que ya han atravesado esta primera capa de seguridad, instalarla fuera del perímetro de seguridad permite identificar eventos que se estén originando desde dentro del Organismo hacia Internet que no hayan sido detenidos por el perímetro de seguridad.

4.3 ¿Qué es el sistema central?

El sistema central se encarga de la recolección de la información que llega de las distintas sondas y de la correlación de eventos para detectar incidentes de mayor nivel de criticidad.

Está compuesto por tres elementos:

- Servidor en tiempo real
- Portal Web de informes estadísticos y detallados sobre los eventos e incidentes detectados.
- Consola de visualización que permite el análisis de los eventos.

4.4 ¿Quién monitoriza el sistema central?

La gestión, actualización y mantenimiento del sistema central está a cargo del CCN-CERT, que con un equipo de expertos en seguridad de la información lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de posibles nuevas fuentes.

4.5 ¿Qué características debe tener el servidor?

La sonda es un servidor de alto rendimiento que va a permitir la recolección de información de la red especificada por el organismo adscrito, filtrado de los eventos específicos de seguridad y su envío al sistema central.

Las características físicas recomendadas del servidor son las siguientes:

Hardware	Descripción
Procesador	Quad Core Xeon 2.5GHz 2x6Mb cache
Memoria	4 GB Memoria RAM
Almacenamiento	2 Discos Duros 146GB 15000 RPM SAS, en RAID 1 (Espejo)
Red	Interfaz/ces de análisis (tantas como redes a analizar): tarjeta/s de red Gigabit Ethernet de tecnología Intel (con driver e1000 o con driver e1000e)
	Interfaz de gestión: tarjeta de red Gigabit Ethernet con distinto driver que la/s interfaz/ces de análisis (p.e. Broadcom…)
Alimentación	2 Fuentes redundantes
Soporte Óptico	Lector de DVD
Sistema operativo	Debian (Instalado por el CCN-CERT)

Los **organismos interesados** en adscribirse a este SAT, **deberán disponer de un servidor** que cumpla como mínimo estas características recomendadas. La **instalación** del sistema operativo, de todas las aplicaciones necesarias y de la securización de la plataforma **se realizará por personal técnico del CCN-CERT** en el momento de la instalación de la sonda en el Organismo.

4.6 ¿Cómo se envían los eventos al sistema central?

El transporte de los eventos se realiza de forma cifrada a través de VPNs y túnel SSL por la salida de Internet del Organismo hacia el Sistema Central, con lo que la confidencialidad e integridad de los envíos queda garantizada.

La conexión entre la sonda individual y el sistema central se puede establecer de dos formas:

- Conexión de la sonda a Internet a través de los Firewall del Organismo adscrito.
- Conexión directa de la sonda a Internet independiente de la red del Organismo.

4.7 ¿Qué información se envía al sistema central?

Las sondas únicamente envían hacia el sistema central alertas generadas tras la detección de algún tipo de evento, definidos en las reglas de detección integradas en el sistema, y que responden a patrones de tráfico potencialmente dañinos o de comportamientos conocidos de determinado tipo de código dañino.

En **ningún momento se realiza un envío del tráfico de Internet del Organismo** hacia el sistema central, manteniéndose así la privacidad en las comunicaciones.

4.8 ¿Qué tipo de ataques puede detectar el SAT de Internet?

La sonda es capaz de detectar todo tipo de ataques y dar una respuesta rápida y eficaz ante cualquier incidente. La información que envían las sondas es posteriormente normalizada en el sistema central, donde se analiza de forma unificada, dando lugar a una correlación avanzada y una mayor fiabilidad en la detección.

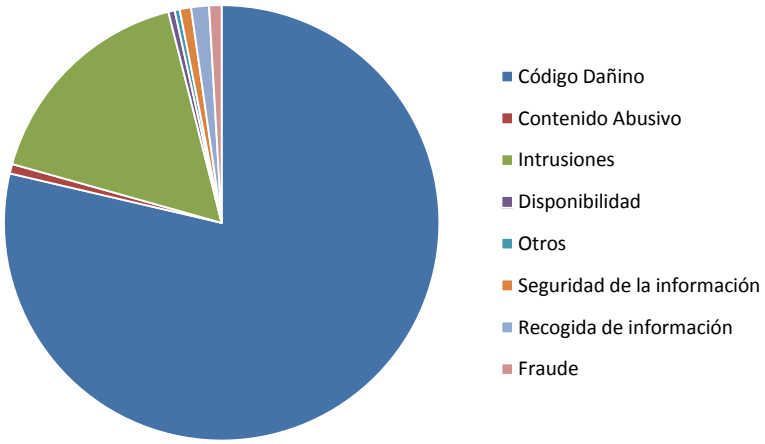

Figura 2. Clasificación y porcentaje de los incidentes notificados

4.9 ¿Qué es el portal del SAT de Internet?

El portal del SAT de Internet es una herramienta con la que el personal TIC del Organismo adscrito puede visualizar en tiempo real los eventos generados por su sonda que se reciben en el sistema central. Además, permite generar reglas de correlación y activar el seguimiento de un evento concreto.

A través del portal el Organismo podrá también gestionar todos los incidentes que le hayan sido notificados, haciendo uso de la herramienta de ticketing utilizada por el CCN-CERT y que ha sido integrada en este portal.

Del mismo modo, también es posible el acceso bajo demanda y en tiempo real a estadísticas e informes sobre el estado general de seguridad de la red.

El acceso a este portal se ofrece al personal TIC una vez se realiza la instalación de la sonda y el Organismo queda adscrito al SAT de Internet.

4.10 ¿Quién realiza la gestión la sonda?

La gestión y administración de la sonda se realiza por el personal técnico del CCN-CERT, para mantener en lo posible un sistema lo más homogéneo posible. Entre las tareas de gestión y administración se incluyen la actualización diaria de las reglas de detección, actualizaciones de sistema operativo, actualización de las aplicaciones, aplicación de parches de seguridad de sistema operativo y de aplicaciones, particularización de las reglas de detección, etc.

4.11 ¿Quién tendrá acceso a la información de mi organismo?

Únicamente tendrán acceso a la información del Organismo adscrito los responsables de la seguridad TIC seleccionados por el propio Organismo para tal efecto y los administradores del sistema, es decir, el equipo de expertos del CCN-CERT que monitoriza el sistema central de sondas. Ninguna otra persona tendrá acceso a esta información. Es importante saber que ningún Organismo tendrá acceso a la información de otros organismos adscritos y **únicamente podrá ver el estado de seguridad de su propia red**, si bien sí que será usada la detección de eventos distribuida para la generación de la inteligencia del sistema de forma automatizada. En este sentido, como en todas las materias competencia del Centro Criptológico Nacional, la política a seguir será mantener en todo momento la confidencialidad de la información tratada.

4.12 ¿Quién se puede suscribir a este servicio?

Cualquier Organismo perteneciente a la Administración Pública o cualquier organización de interés estratégico para el país puede adherirse al Sistema de Alerta Temprana de Internet, contactando con el CCN-CERT.

4.13 ¿Qué información voy a recibir si estoy adscrito al SAT de Internet?

El Organismo que esté adscrito al Sistema de Alerta Temprana de Internet, recibirá periódicamente informes especializados, de alto nivel y sensibilidad, que capacitarán al personal responsable de la seguridad TIC del Organismo para tomar las decisiones pertinentes y disponer de la información necesaria para conocer el estado de seguridad de su red y las necesidades de la misma. Entre otra información, los informes incluyen el código dañino y los ataques detectados en cada Organismo, los incidentes gestionados en un período de tiempo, las IPs de origen y destino y un listado de todos los incidentes pendientes de resolver.

Del mismo modo, anualmente recibirá un informe en el que se describirá el nivel de amenaza de la red durante ese periodo e indicadores que permitirán valorar tanto el servicio ofrecido por el SAT como la capacidad de respuesta del Organismo en la resolución de los incidentes de seguridad gestionados.

4.14 ¿Cómo voy a recibir la información de los incidentes?

Para la recepción de los incidentes el Organismo que esté adscrito al Sistema de Alerta Temprana de Internet deberá de disponer de una cuenta de correo a la que enviar la notificación de los incidentes de seguridad. Esta cuenta de correo deberá ser única, por lo que se recomienda al Organismo la creación de una lista de distribución que reciba todo el personal TIC que vaya a encargarse de la investigación de los incidentes de seguridad.

La información referente a los incidentes de seguridad detectados por el personal técnico del CCN-CERT estará disponible en el portal del SAT de Internet, al que tendrán acceso los responsables de seguridad de los Organismos adheridos a este servicio, donde podrán realizar el seguimiento de los incidentes notificados y donde podrán informar de las acciones llevadas a cabo para la resolución del mismo.

En este sentido, para el intercambio de información referente a los incidentes de seguridad, y en previsión de la necesidad de intercambio de información sensible en respuesta a la investigación de los incidentes, será necesario que el organismo genere un par de claves PGP/GPG para intercambiar información de manera cifrada en el caso que fuese necesario.

Una vez generadas las claves PGP/GPG asociadas a esta cuenta de correo, el Organismo deberá remitir al CCN-CERT la clave pública para poder cifrar la información que éste quisiera remitir de manera cifrada. Del mismo modo, el CCN-CERT proporcionará la clave pública de la cuenta de correo utilizada para la notificación de incidentes para que el Organismo pueda también enviarle información cifrada en caso necesario.

5. CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como CERT Gubernamental/Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

6. PUNTO DE CONTACTO

- Tfno. 91 283 2329 / 91 283 2251
- Web: https://www.ccn-cert.cni.es
- E-Mail: sondas@ccn-cert.cni.es