CARTA LOCAL

REVISTA DE LA FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

www.femp.es | Febrero 2016

COLABORACIÓN

SAT-INET: detección de ciberincidentes en las Entidades Locales

La interrupción y toma de control de los sistemas de un Ayuntamiento; el secuestro y cifrado de los archivos de un equipo con la exigencia del pago de un rescate; la sustracción, publicación o venta de información sensible o la desfiguración de la página web de un Consistorio, son algunos de los incidentes que, diariamente, reciben las Entidades Locales de nuestro país.

CNI-CERT

Ante la intensidad y sofisticación de estos ciberataques, el Centro Criptológico Nacional (CCN), a través de su Capacidad de Respuesta a Incidentes (CCN-CERT), y de acuerdo a la normativa y legislación vigente, ofrece a todas las Administraciones Públicas (incluida la Local) una serie de servicios con los que afrontar de forma activa estas amenazas. Entre otros, su Sistema de Alerta Temprana en Internet (SAT-INET), al que ya están adscritos 89 organismos (entre ellos diez Ayuntamientos) que se benefician de las ventajas de un servicio de prevención y detección de ciberataques.

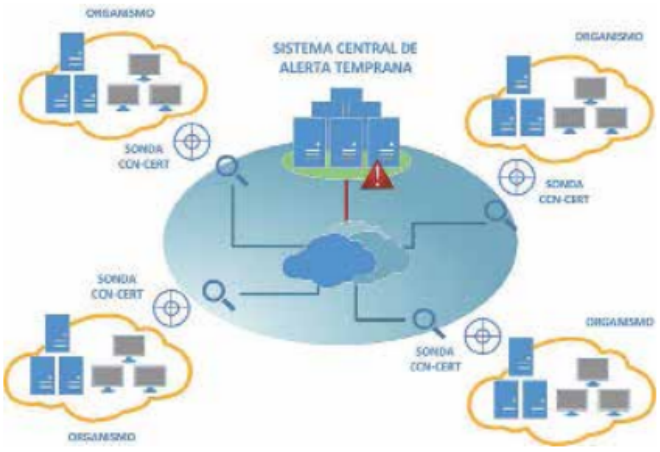
Durante el año 2015, el Centro Criptológico Nacional (CCN), y su Capacidad de Respuesta a Incidentes (CCN-CERT), gestionó 18.232 ciberincidentes, lo que representa un incremento cercano al 42% con respecto al año 2014 y que supone cerca de 50 ataques diarios. De ellos, 430 fueron considerados con un nivel de riesgo de muy alto o crítico; es decir se tuvo constancia de que el ataque afectó a los sistemas del organismo y a su información más sensible.

La introducción de código dañino en los sistemas (con niveles muy bajos de detección por parte de las empresas antivirus), las intrusiones mediante ataques a páginas web con el fin de robar información sensible, así como el secuestro del ordenador o el cifrado de sus archivos (ransomware) con la exigencia de un rescate, fueron algunos de los incidentes más recurrentes sufridos por nuestra Administración. Unas Administraciones que, no lo olvidemos, dependen del uso de Internet y de las nuevas tecnologías, tanto para su funcionamiento interno como para los servicios que prestan a la población (más del 95% de los servicios públicos ya están operativos a través de Internet).

Ante esta situación, la labor del CCN ha ido encaminada desde su creación en el año 2002, en el seno del Centro Nacional de Inteligencia (CNI), a reducir los riesgos y amenazas provenientes del ciberespacio, adecuándose a los nuevos desafíos y buscando, a través de las funciones que tiene encomendadas por ley, prevenir su propagación y atajar su impacto de la forma más rápida posible. Para ello, ha venido potenciando sus acciones, no sólo defensivas, sino primordialmente preventivas, correctivas y de contención. A través de su equipo de expertos destinados a investigar sobre técnicas empleadas, funcionamiento de los ataques, soluciones y procedimientos más adecuados para hacerlos frente, el CCN-CERT ofrece todos sus servicios a las Administraciones Públicas, entre los que destaca su Sistema de Alerta Temprana (SAT), tanto en Internet como en la red SARA.

SAT-INET, anticiparse al atacante

En el año 2008, el CCN-CERT, y con el fin de detectar cuanto antes cualquier tipo de ataque o anomalía en los sistemas de la Administración Pública, inició el desarrollo de su Sistema de Alerta Temprana (SAT). En un primer momento, este servicio comenzó con la monitorización de la Red de Intercomunicación de todos los organis-

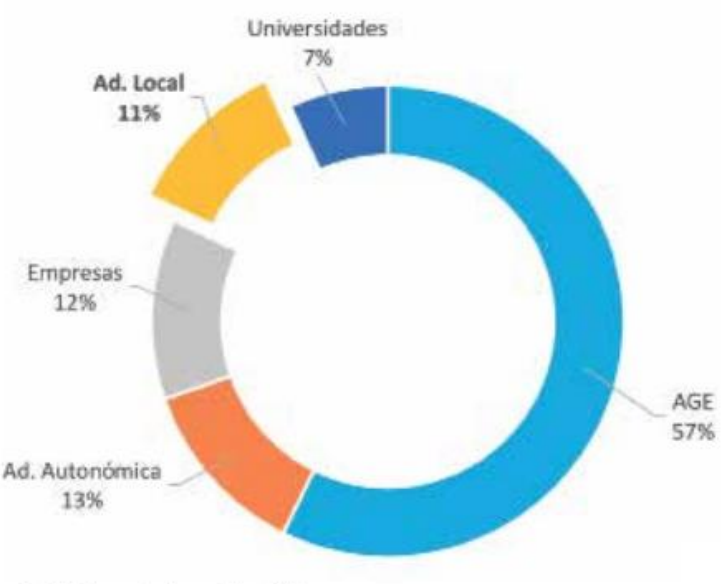


Sistema de Alerta Temprana en Internet (SAT-INET) del CCN-CERT.

mos 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 CCN-CERT, 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.

A este servicio puede adherirse cualquier organismo público que lo solicite, entre ellos las Entidades Locales. De hecho, desde su puesta en marcha, ya son 89 las organizaciones adscritas al sistema (10 Ayuntamientos), que se benefician de este servicio de prevención y detección de incidentes.



Tipología de las organizaciones adscritas al SAT.

Beneficios para las Entidades Locales

Solicitar la adhesión al SAT-INET representa para cualquier Entidad Local una serie de ventajas que podrían resumirse en los siguientes puntos:

- Detección de todo tipo de ataques e incidentes y, con ello, una respuesta rápida y eficaz a los incidentes.
- Correlación: no sólo se detectan incidentes importantes de forma individual, sino que se pueden detectar eventos más complejos que involucren 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.
- Soporte a la resolución de incidentes. Como CERT Gubernamental nacional 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.
- 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.

La Entidad Local que desee recibir más información sobre el SAT del CCN-CERT y los beneficios de su implantación, puede realizar sus consultas a través de la cuenta de correo electrónico:
sat-inet@ccn-cert.cni.es
Y en la web: www.ccncert.cni.es

CCN-CERT, principal línea de defensa frente a las ciberamenazas en la Administración

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (organismo adherido al Centro Nacional de Inteligencia). Este servicio se creó en el año 2006 como el CERT Gubernamental/Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas clasificados, de las Administraciones Públicas (Central, Autonómica y Local) 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.