GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
Centro Criptológico Nacional

IV JORNADA STIC CCN-CERT

Riesgos emergentes en las AAPP:

el ENS y los requisitos mínimos para hacerles frente

Introducción

El uso de las TIC en la Administración Pública española ha ido incrementándose significativamente en los últimos años hasta ocupar, según el informe *EGoverment Readiness* de Naciones Unidas, la novena posición del mundo en Administración Electrónica. Sin duda, la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos, ha impulsado esta situación y ha obligado a las administraciones públicas a conjugar la prestación de más y mejores servicios con la generación de confianza en los medios electrónicos. Pero este desarrollo de la e-Administración, lleva aparejada ineludiblemente un mayor riesgo de sufrir ciberataques que pongan en peligro la seguridad de la información y los servicios ofrecidos a los ciudadanos.

De hecho, si por algo se ha caracterizado el panorama mundial en los últimos meses, es por la creciente preocupación de los gobiernos en implementar y mejorar las políticas y capacidades de seguridad, invirtiendo en recursos y elaborando estrategias nacionales de **ciberseguridad**, que aborden el problema de un modo global. Porque, sólo desde una política global y definida se puede luchar contra la evolución constante de las herramientas dañinas, el incremento de vulnerabilidades zero-day, los métodos innovadores para controlar sus botnets por parte de los hackers, la distribución de código dañino a través de redes sociales, la manipulación de los sistemas de optimización de los motores de búsqueda, los ataques con motivo político y/o propagandístico bajo la forma de ataques DDoS o, llegando más lejos, los ciberataques a las infraestructuras críticas de un país.

La experiencia de más de cuatro años del **CCN-CERT** como Capacidad de Respuesta ante Incidentes de Seguridad y como CERT Gubernamental encargado de velar por la seguridad de los sistemas de toda la Administración, corrobora esta necesidad de contar con una visión holística, que incluya medidas tanto preventivas como reactivas. Medidas que sean capaces de reaccionar ante el constante incremento de incidentes y, sobre todo, que prevengan su propagación y atajen su impacto de la forma más rápida posible. Ya no basta con responder y gestionar el incidente una vez se haya 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 y evitar su propagación a través de Internet.

Algunas de estas acciones se han ido adoptando ya. Así, el **Esquema Nacional de Seguridad** (de cuya regulación a través del RD 3/2010, de 8 de enero, se cumple casi un año) ha venido a plasmar en un documento un conjunto homogéneo y compacto de medidas de seguridad que, una vez se apliquen, mejorarán considerablemente los niveles de seguridad de los distintos organismos de la Administración.

Por su parte, el CCN-CERT ha desarrollado el **Sistema de Alerta Temprana** para la detección rápida de incidentes y anomalías dentro del ámbito de la Administración (de la red SARA y de

los accesos a Internet de los distintos organismos) que permite detectar todo tipo de ataques, evitando su expansión, respondiendo de forma rápida ante el incidente detectado y, de forma general, generando normas de actuación para evitar futuros incidentes.

De igual forma, es necesaria la puesta en común de conocimientos, el análisis de las principales amenazas existentes en la actualidad y el estudio de las últimas novedades en herramientas y soluciones que hagan frente a los ciberataques y que garanticen la seguridad en los sistemas TIC de la Administración. Este es y ha sido el principal objetivo de las Jornadas organizadas por el CCN-CERT, que este año celebran su cuarta convocatoria, y que espera acoger, al igual que en ediciones anteriores, a los mayores expertos en la materia y los principales representante de las distintas AAPP (general, autonómica y local).

Así pues, la **IV Jornada STIC CCN-CERT**, que tendrá lugar el **14 de diciembre**, en el Centro Superior de Estudios de la Defensa Nacional (**CESEDEN)**, en Madrid, volverá a convertirse en la cita ineludible para todos los responsables TIC de la Administración.

Beneficios del patrocinio

Durante el día en el que se celebra esta IV Jornada, los asistentes tienen una oportunidad única de comunicarse con los principales responsables de seguridad de la Administración Pública española (general, autonómica y local) y contactar con ponentes y asistentes de reconocido prestigio, con los que compartir experiencias, conocimientos e inquietudes.

Patrocinar las IV Jornada STIC CCN-CERT, representa para una compañía o institución:

- Acceso único a los principales responsables de seguridad de la Administración Pública.
- Distinguirse como colaborador del CCN-CERT.
- Posicionarse como empresa comprometida en la Ciberseguridad
- Visibilidad exterior a través de la comunicación a los medios que se realizará del evento.

Categorías de patrocinio

Las distintas categorías de patrocinio fijadas cuentan con una serie de prestaciones, adecuadas al coste de las mismas y a los compromisos adquiridos por cada una de las partes.

1. Platinum: Máximo 2

Esta categoría incluye:

- Cartel expositor de la empresa en la entrada de las jornadas/comida
- Logotipo tamaño XL en la contraportada del programa informativo
- Logotipo tamaño XL en las ponencias
- Logotipo tamaño XL en carpeta entregada a todos los asistentes
- Logotipo tamaño XL con enlace y texto de la empresa en la página web del evento
- Entrega de documentación de la empresa a todos los asistentes (soporte papel y/o electrónico)
- Entrega de regalo promocional a los asistentes (optativo)
- 3 inscripciones del personal de la empresa (con almuerzo incluido)
- 5 invitaciones a clientes (sólo de AAPP y no intercambiable por personal de la empresa) Límite: 30 de noviembre
- Notas de prensa/material promocional de la empresa:
    - Insertada en la página web del evento (nota de prensa)

Aportación: 6.500 € + 18% IVA = 7.670 €

Gold: Máximo 4

Esta categoría incluye:

- Logotipo tamaño L en la contraportada del programa informativo
- Logotipo tamaño L en las ponencias
- Logotipo tamaño L en carpeta entregada a todos los asistentes
- Logotipo tamaño L con enlace y texto de la empresa en la página web del evento
- Entrega de documentación de la empresa a todos los asistentes (soporte papel y/o electrónico)
- Entrega de regalo promocional a los asistentes (optativo)
- 2 inscripciones gratuitas (con almuerzo incluido)
- 3 invitaciones a clientes (sólo de AAPP y no intercambiable por personal de la empresa) Límite: 30 de noviembre
- Notas de prensa/material promocional de la empresa:
    - Insertada en la página web del evento (nota de prensa)

Aportación: 3.500 € + 18% IVA= 4.130 €

Silver: Máximo 8

Esta categoría incluye:

- Logotipo tamaño M en la contraportada del programa informativo
- Logotipo tamaño M en las ponencias
- Logotipo tamaño M con enlace y texto de la empresa en la página web del evento
- Entrega de documentación de la empresa a todos los asistentes (soporte papel y/o electrónico)
- Entrega de regalo promocional a los asistentes (optativo)
- 1 inscripción gratuita (con almuerzo incluido)
- 2 invitaciones a clientes (sólo de AAPP y no intercambiable por personal de la empresa). Límite: 30 de noviembre

Aportación: 2.000 € + 18% IVA = 2.360 €

Términos y Condiciones del Patrocinio

Todas las empresas que deseen acogerse a cualquiera de las modalidades de patrocinio anteriormente expuestas deberán formalizar la petición antes del **25 de noviembre de 2010** y hacer efectivo el pago del mismo con anterioridad a la celebración del evento.

La coordinación del evento deberá contar con toda la información, en tiempo y forma, necesaria para poder cumplir con sus compromisos adquiridos hacia los patrocinadores (logotipos, material promocional, regalos, notas de prensa, etc.).

Contacto

Para reservar o solicitar más información sobre los patrocinios disponibles o sobre la inscripción a la Jornada, póngase en contacto con:

TB·Security
Tel. (+34) 91 301 34 95
eventos@ccn-cert.cni.es