

Copatrocinan:



Organiza:



El papel del analista, la tecnología y la inteligencia

El replanteamiento de la ciberseguridad ante los ataques que nos vienen



25 octubre_2016

Madrid. Hotel Novotel
Campo de las Naciones

www.revistasic.com/tendenciassic

tendencias





David Barroso
CounterCraft



Román Ramírez
Ferrovial

Ataque y defensa: qué está cambiando en la ciberseguridad

La ciberseguridad está sometida a la dinámica que se crea con la confrontación de los que atacan y los que se defienden. Y ello obliga a ahondar, cada cierto tiempo, en los cambios que se están produciendo en la naturaleza y formas de los ataques, que abocan a un replanteamiento de la gestión de riesgos, a la puesta en práctica de fórmulas más eficientes de automatización de las defensas en “tiempo real”, a la valoración de los analistas y a la profundización de sus habilidades en ese territorio sin límites (salvo los marcados por las leyes) que es el análisis de macrodatos, lamentablemente también colonizado por la delincuencia.

La modificación del escenario que está produciendo esta fase del proceso de transformación, sugiere la necesidad, también, de transformar la ciberseguridad. Uno de esos cambios es el de la obligatoriedad de la notificación de incidentes, que en pocos años se convertirá en norma general, ya afecte o no a datos personales. Este hecho obliga a empresas y a administraciones públicas a tener perfectamente ajustado, y al día (es decir, teniendo en cuenta el estado del arte de la tecnología y el valor de lo protegido), su sistema de ciberseguridad.

Tendencias SIC propone un debate en el que expertos técnicos –Román Ramírez (Ferrovial) y David Barroso (CounterCraft), y de compañías proveedoras de soluciones tecnológicas punteras (FireEye, Fortinet, IBM, Palo Alto Networks, Panda Security, Symantec y Trend Micro)– expondrán su visión específica de la evolución de atacantes y ataques, más allá del *malware*, explicarán las nuevas líneas en la ciberdefensa que están investigando sus laboratorios y equipos de especialistas, y los efectos que esto está teniendo en la evolución de enfoque en sus herramientas.

Al tiempo, Tendencias SIC contará también con la participación de representantes de dos CERTs españoles de referencia, el CCN-CERT y el CERTSI, que desempeñan un papel esencial en la vertebración y modernización de la ciberseguridad.



Álvaro García
FireEye



Ignacio Franzoni
Fortinet



Alberto Benavente
IBM Security



Jesús Díaz
Palo Alto Networks

PROGRAMA



09:00h. Acreditación

EL REPLANTEAMIENTO DE LA CIBERSEGURIDAD

09:15h. **El papel del analista, la tecnología y la inteligencia. Otras maneras de defensa**
David Barroso
CEO de **Countercraft**

09:45h. **El papel del analista, la tecnología y la inteligencia. La necesidad de un nuevo enfoque**
Román Ramírez
Responsable de Arquitectura de Seguridad de **Ferrovial**

10:15h. Coloquio

HALLAZGOS Y PREVISIONES DE LA INDUSTRIA

10:20h. **FireEye**
Álvaro García
Ingeniero de Sistemas Iberia

10:40h. **Fortinet**
Ignacio Franzoni
Ingeniero de Sistemas Senior

11:00h. **IBM Security**
Alberto Benavente
Responsable de Soluciones de Seguridad

11:20h. Pausa-café

11:50h. **Palo Alto Networks**
Jesús Díaz
Ingeniero de Sistemas Senior

12:10h. **Panda Security**
Raúl Pérez
Global Presales Manager

12:30h. **Symantec**
Miguel Suárez
Responsable de Preventa para España e Italia

12:50h. **Trend Micro**
José de la Cruz
Customer Service Manager

DEBATE

13:10h. Coloquio general con los representantes de la industria, al que se incorporan:
Javier Candau
Jefe del Departamento de Ciberseguridad del **Centro Criptológico Nacional-CCN**
Javier Berciano
Coordinador de Operaciones del CERTSI. **INCIBE**

14:15h. Almuerzo para los asistentes



Raúl Pérez
Panda Security



Miguel Suárez
Symantec



José de la Cruz
Trend Micro



Javier Candau
Centro Criptológico Nacional-CCN



Javier Berciano
INCIBE

CCN-CERT

Un año más, el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional ha informado que, en 2015, se gestionaron en España 18.232 incidencias cibernéticas, lo que supone un 41% más que en 2014. De todas ellas, 430 se han clasificado con un nivel de peligrosidad “muy alto” o “crítico”. El ciberespionaje, la ciberdelincuencia y el *hacktivismo* han sido las principales amenazas que más han desafiado a la seguridad del ciberespacio, pero, este año, el CCN ha querido acentuar también la amenaza que supone el ciberyihadismo.

INCIBE

Según datos del estudio “Tendencias en el mercado de la Ciberseguridad” que ha elaborado el Instituto Nacional de Ciberseguridad (INCIBE), el sector tiene una previsión de aumento de la demanda que alcanzará los 79.292 millones de euros en 2018. Son varias las tendencias ciber que se destacan en el estudio: la protección de las redes industriales inteligentes y Smart Grids, la seguridad en los servicios Fintech o la protección de sistemas de comunicación vía satélite y drones.

SYMANTEC

Especial relevancia cobra el sector financiero que, en 2015, experimentó un aumento de los ataques dirigidos. Un informe llevado a cabo por Symantec también alude a los servicios online como las redes sociales, casas de subastas, y servicios de correo web como otros de los sectores más atacados.

BLUE COAT

Un estudio de Blue Coat alerta de los peligros del Shadow Data, todo aquel contenido descontrolado que los empleados almacenan y comparten mediante aplicaciones en la nube. De las más de 15.000 aplicaciones empresariales en la nube analizadas y de 108 millones de documentos almacenados y compartidos en ellas, se ha comprobado que el 99% no contenían suficiente seguridad, controles de cumplimiento y otras características para proteger los datos de la empresa en la nube de forma efectiva.

IBM

Resultan llamativos los datos de una reciente investigación de IBM de la que se desprende que el 68% de los CEOs son reacios a compartir externamente información de su organización relativa a los incidentes sobre ciberseguridad, mientras que los ciberdelincuentes siguen perfeccionando su capacidad para compartir información en tiempo real a través de la *Dark Web*.

PALO ALTO NETWORKS

Un informe llevado a cabo por Ponemon y Palo Alto Networks y realizado a 300 participantes Estados Unidos, Alemania y Reino Unido –los cuales afirmaban tener experiencia penetrando en sistemas informáticos– revela que el 69% de los ciberdelincuentes actúan por dinero y no por reputación o cuestiones geopolíticas.

TREND MICRO

De acuerdo con el estudio “The trouble at your door”, realizado por Trend Micro, España está entre los países de la UE más afectados por los ciberataques dirigidos. Las organizaciones españolas están sufriendo algunas de las peores pérdidas de datos que se están produciendo en Europa, estando relacionadas en su mayoría con el robo de tarjetas de crédito y datos personales, con un coste asociado en cada una de las empresas afectadas de aproximadamente un millón de euros.

PANDA SECURITY

Panda Security recoge, además, la realidad de las pequeñas y medianas empresas españolas en materia de seguridad informática. De acuerdo con el estudio el “Estado de Protección en las Pymes”, en 2015, el 91% de las pymes españolas afirmaba sufrir ataques informáticos a diario.

FORTINET

En “The Evolving Threat Landscape”, Fortinet alerta sobre las consecuencias de quedarse atrás en la carrera de la ciberseguridad. Se esperan más de 20.000 millones de dispositivos conectados en los próximos 4 años, lo que obligará a individuos y organizaciones a hacer frente a una superficie de ataque en expansión y carente de fronteras. Un escenario muy complejo, cuando, precisamente, la complejidad es el peor enemigo de la seguridad.

FIREEYE

De acuerdo con el reciente estudio “M-Trends 2016”, la media del número de días que los atacantes están presentes en la red de su víctima, antes de ser descubiertos, bajó de 205 días en 2014 a 146 días en 2015. Sin embargo, algunas brechas de seguridad pueden no ser detectadas durante años. Además, dichas brechas continúan siendo descubiertas en su mayoría por terceros.



FECHA Y LUGAR

25 de octubre de 2016
Hotel Novotel.
Campo de las Naciones
C/ Amsterdam, 3.
28042 Madrid

ORGANIZA

Revista SIC. Ediciones CODA
C/ Goya, 39. 28001 Madrid
Tel.: 91 575 83 24
info@revistasic.com
www.revistasic.com

SOLICITUD DE INSCRIPCIÓN GRATUITA

El procedimiento para la solicitud de la inscripción es vía web mediante la cumplimentación de un formulario. Al ser el aforo limitado, la inscripción se cursará por riguroso orden de fecha de entrada de solicitud.

Sitio web: www.revistasic.com/tendenciassic

- Una vez realizada la solicitud, la organización le informará –por razones de limitación del aforo– si ha quedado inscrito o no.
- En ningún caso se admitirán más de tres inscripciones de profesionales de una misma compañía.