Oracle celebra una jornada sobre seguridad cloud

21/04/2017 http://www.redseguridad.com/actualidad/info-tic/oracle-celebra-una-jornada-sobre-seguridad-cloud

Con el objetivo de profundizar en la necesidad de proteger la nube, la compañía Oracle celebró en Madrid una jornada denominada Oracle Cloud Security Day. En ella dio a conocer a los asistentes su propuesta tecnológica en este sentido, además de contar con otros ponentes que incidieron en la necesidad de extremar la protección de los sistemas y los dispositivos por parte de las organizaciones.

El director de Ventas de Seguridad de Oracle, Mauricio Gumiel, fue el encargado de abrir este evento haciendo hincapié en la importancia que hoy en día tiene la seguridad en los procesos de transformación digital de las empresas. Ahora bien, con la llegada de nuevas tecnologías, como la robótica, la inteligencia artificial, el IoT, etc., “es preciso implementar medidas de seguridad más sofisticadas”, en palabras del directivo. Una prueba de ello es el aumento del número y la complejidad de los ciberataques, cuyo principal objetivo es robar datos a las empresas. Por eso, a juicio de Gumiel, “tenemos que ponernos de acuerdo sobre cómo vamos a defendernos, y qué medidas inteligentes y personalizadas debemos tomar para ello”. En este sentido, asegurar los datos empresariales contenidos en la nube se convierte en una prioridad fundamental.

Precisamente, para dar a conocer la propuesta de Oracle en este ámbito, a continuación, tomó la palabra David Núñez, consultor de ventas de la compañía, quien comenzó su intervención mostrando algunos datos interesantes. Por ejemplo, según el directivo, el 91% de las empresas tiene preocupaciones de seguridad

al adoptar la nube pública. A pesar de ello, cada vez hay más información en el cloud. “Incluso, muchas empresas cuentan con recursos en la nube de los que ni siquiera el departamento de TI tiene constancia. Es lo que se denomina el Shadow IT”, explicó.

Para intentar poner orden en todo esto, el directivo presentó la estrategia de seguridad de Oracle, que se basa en seis pilares: Identity cloud service, Security monitoring and analytics cloud service, CASB cloud service, API Platform cloud service, Compliance cloud service e Hybrid data security protection: database security. Con todo ello se pretende tener una visibilidad amplia de los sistemas mediante un cuadro de control central, establecer políticas de acceso e identificación de los usuarios, llevar a cabo las medidas de cumplimiento necesarias, proteger los datos y tener la capacidad de responder a las amenazas existentes.

Seguidamente, intervino Silvia Barrera, inspectora de la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía, que inició su ponencia confirmando que, hoy en día, la ciberdelincuencia mueve más dinero que el narcotráfico en el mundo. Sin embargo, los usuarios no son conscientes de los riesgos reales que acarrea. Y de ello, en parte, se valen los cibercriminales. Según Barrera, “cometer delitos en este ámbito es un negocio: se puede hacer desde cualquier parte del mundo, llegas a millones de víctimas, con un riesgo personal de cero y con unas ganancias cuantiosas”, explicó. De hecho, la inspectora puso el ejemplo del phishing, “con el que entre un 1% y un 5% cae en la trampa”. Y añadió: “El 95% de las incidencias ocurren porque nosotros les facilitamos a los hackers que ocurran”. Precisamente, la inspectora confirmó que muchas empresas no cuentan todavía con protocolos de seguridad apropiados y no saben a quién acudir en caso de tener un problema. Por eso, y partiendo de la base de que “la información es el oro del siglo XXI”, según afirmó, hay que acabar con el desconocimiento existente, porque, en el ámbito de la seguridad, “la responsabilidad es de cada uno de los usuarios”, concluyó.

Otro de los ponentes en tomar la palabra fue Francisco Lázaro, director del Centro de Estudios de Movilidad e Internet de las Cosas de ISMS Forum. El directivo abordó el tema de la seguridad en los entornos IoT, cada vez más necesaria con la proliferación de todo tipo de dispositivos conectados. De hecho, esto, según Lázaro, “va a suponer un cambio importante en la sensibilidad de las personas, porque se van a ver afectadas”. Para demostrarlo, puso como ejemplo el entorno de la salud, en el que están apareciendo dispositivos como pulseras o relojes que permiten monitorizar la salud, productos médicos implantables, medicamentos ingeribles inteligentes, productos portables externos y equipos estacionarios. Todos ellos pueden ser objetos de brechas de seguridad o vulnerabilidades. Por tanto, según Lázaro, es importante que “los fabricantes de productos IoT incorporen la seguridad desde su diseño”, porque, si no es así, se pueden producir bastantes riesgos como fallos operacionales en los objetos, daños en la privacidad o ataques a terceros, entre otros. Y a ello, además, deben ayudar también las administraciones, desarrollando normativas y exigencias que regulen esta necesidad.

La jornada concluyó con las intervenciones de Maica Aguilar, awareness, audit y compliance de Ferrovial; y Luca Martelli, director de Soluciones de Identidad y Seguridad de Oracle; así como con la mesa redonda sobre inteligencia digital, en las que estuvieron presentes representantes de Accenture, CMC, Capgemini, Everis e IECISA.