# Las brechas de seguridad en IoT son pasarelas para la extorsión o ataques tipo 'DDoS'

**Tags:** Seguridad Ciberseguridad

**Alfonso Casas 19 octubre 2017** http://cso.computerworld.es/cibercrimen/las-brechas-de-seguridad-en-iot-son-pasarelas-para-la-extorsion-o-ataques-tipo-ddos

**Dentro del marco de la segunda edición del Foro de la Movilidad e IoT que ha tenido lugar en Madrid, organizado por ISMS Forum, se han abordado interesantes aspectos relacionados con este ecosistema de dispositivos interconectados y su seguridad.**


Desde las **implicaciones en materia de seguridad y privacidad**, hasta el **análisis de los vectores** de ataque empleados hasta ahora, durante la jornada, fueron abordados aspectos como el impacto que provocan estas tecnologías en las organizaciones, y los retos a los que se enfrentan las empresas **en materia de protección y prevención.**

De especial interés resultó **la mesa redonda donde se dieron cita portavoces** de compañías como **Kaspersky Lab, Akamai, HPE y Prosegur.** Los participantes admitieron estar de acuerdo en que hechos como **el *time to market* asociado a la fabricación y comercialización de nuevos productos IoT** propicia que se produzcan situaciones de grave riesgo en **ciberseguridad.**

Para **José María Cayuela, Security Specialist Senior de Akamai**, "el tráfico procedente de productos **IoT** ha crecido un 70% por lo que era de esperar que se produjeran ataques valiéndose de estos dispositivos, como los de denegación de servicio distribuido". Desde **Akamai**, afirma Cayuela, "abogamos por la elaboración de patrones y buenas prácticas que informen de los dispositivos que carecen de **políticas de seguridad"**. La compañía ha presentado recientemente **su nuevo servicio** en el que plantea que cada dispositivo se conecte con la nube y esté identificado para garantizar unas comunicaciones seguras.

Por su parte, **Dani Creus, Senior Security Research de Kaspersky Lab**, se muestra tajante al afirmar que "la brecha dejada por estos **dispositivos IoT**, abre las puertas a otras amenazas y a que se produzcan nuevos ataques". Es por ello que **desde Kaspersky planteamos entornos de seguridad robustos** para áreas determinadas como el de Industria, creando un sistema operativo propio **Kaspersky OS** que no tenga las vulnerabilidades intrínsecas que tienen los sistemas heredados", puntualiza Creus.

**Jorge Laredo, Pointnet Cosulting Manager de HPE** destaca que “es necesario diseñar una estructura de seguridad teniendo en cuenta que todas las empresas tendrán, antes o después, dispositivos IoT en su organización. Es por ello que hace falta aplicar medidas de regulación, concienciación y conocimiento”.

**Fernando Romero Horcajada, Global Architecture Responsible de Prosegur** hizo referencia a la necesaria ciberseguridad desde la fase de diseño, a lo que añadió que “es muy importante llevar a cabo auditorías para **detectar las vulnerabilidades de los dispositivos** que son adquiridos, así como mantener el hábito de actualización durante todo el ciclo de vida de los mismos”.

Como conclusión de esta mesa redonda del **II Foro de la Movilidad e IoT**, cabe destacar, que es de obligado cumplimiento el que se tomen **medidas y normas de buena gobernanza** para garantizar la disponibilidad, la configuración y el despliegue de actualizaciones. Ahora bien, la regulación no debe verse como una medida a cumplir por imposición, pues esto puede propiciar que no se desarrollen otras acciones de defensa. **Los ataques a dispositivos IoT afectarán al bienestar de las personas**, con lo que se hace necesaria **una regulación que marque jurisprudencia**, dictando culpabilidades y depurando responsabilidades en el caso de que se produzcan incidentes.