¿El internet de las cosas es seguro?

Por: David Acosta, Consultor y conferencista mundial en temas de seguridad.

La base del "Internet de las cosas" (Internet of Things – IoT) es la identificación de activos físicos y sus características empleando sensores para que puedan ser representados en un ambiente digital. La aplicación de este concepto conlleva una serie de mejoras en el análisis de patrones de datos con el fin de optimizar los tiempos de respuesta en la toma de decisiones a niveles cercanos al tiempo real. Ejemplos claros se pueden encontrar en la industria de manufactura, automovilística, agricultura, domótica, salud, entre otros. No es un concepto nuevo, de hecho su implementación genérica se puede encontrar en sistemas de automatización y control (SCADA - supervisory control and data acquisition).

La masificación de Internet, la implementación de interconexión entre dispositivos de la vida diaria (electrodomésticos, automóviles, sistemas de domótica, teléfonos móviles, etc.), la computación en la nube, el decremento en los costes de almacenamiento y procesamiento y el impacto de IPv6 han dado pie a que este concepto deje de ser una idea puramente teórica a tener un potencial impacto de entre 30 y 50 billones de dispositivos interconectados en el 2020 (según Gartner y Cisco, respectivamente).

Sin embargo – y al igual que todas las tecnologías – su masificación entra en conflicto con los niveles de seguridad implementados, ya que para que haya una adopción global por lo general se opta por sacrificar seguridad por operatividad. Si no se cambia ese paradigma en este momento, en un futuro cercano no podremos tener los niveles de madurez en seguridad que permitan la gestión de unos niveles de riesgo homogéneos y tolerables y se tendrá que optar por la aplicación de "parches" reactivos, lo cual puede ser el freno de tal crecimiento desmedido.

¿Pueden crearse ataques dirigidos a M2M?

El IoT está basado en tecnologías existentes que no están exentas de vulnerabilidades. La integración e interconexión de todos estos elementos conlleva a una sumatoria de riesgos que simplemente cambiarán el escenario de ataque pero los conceptos de amenaza y vulnerabilidad seguirán siendo los mismos, afectando – como siempre - la confidencialidad, la integridad y la disponibilidad:

Confidencialidad: Dado que uno de los objetivos principales del M2M es la identificación de elementos y sus características (ubicación, velocidad, humedad, temperatura, etc.), dichos datos al ser conocidos por personal no autorizado pueden impactar la privacidad de los elementos monitorizados.

Integridad: La manipulación no autorizada de datos de IoT pueden afectar o distorsionar las conclusiones del análisis que da paso a la toma de decisiones. Esto se convierte en un tema más crítico cuando dichas conclusiones son tomadas en tiempo real.

Disponibilidad: Los ataques de denegación de servicio contra sensores y lectores (que son elementos con poco nivel de procesamiento y energía limitada), sistemas de análisis y captura, sistemas de almacenamiento y la saturación de redes de comunicaciones afectarán la respuesta inmediata que se espera de estos sistemas. Así mismo, redes zombi conformadas por dispositivos con bajo poder de procesamiento pero con conexión a una red global estarán listos para asediar un objetivo específico.

Estamos frente a la evolución natural del Internet que conllevará una serie de beneficios tangibles en la vida diaria, pero dicha tecnología arrastrará consigo una serie de riesgos que ya conocemos y que su impacto podrá ser amplificado si no se implementan los controles necesarios. En mi opinión, el "Internet de las cosas" es solo otro nombre rimbombante en la evolución de un concepto que ya conocemos y que estamos a puertas de su masificación, al igual que sucedió con la "computación en la nube", solo que el momento adecuado es aquí y ahora. El escenario está dispuesto, solo falta que se lance el primer ataque…