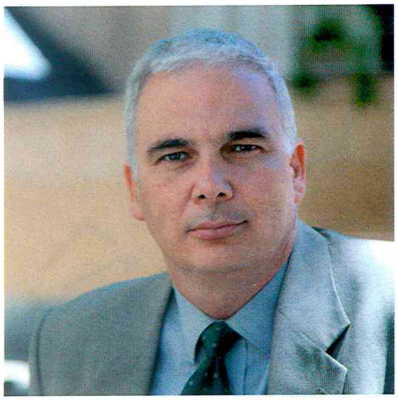
Internet de las cosas: pase hasta la cocina



Francisco Lázaro
Director del Centro de Estudios de Movilidad e IoT del ISMS Forum (CEM)

Paloma LLaneza
Comité Operativo del CEM

Internet de las cosas, Internet de las casas, Internet de las personas, Internet de la web, Internet del todo, Internet de los servicios, ciudades inteligentes, industria 4.0... Tantos términos para extender la visión de un mundo conectado, absolutamente conectado. Y no hablamos de otros mundos, todos y cada uno están en éste, con un grado de conexión sin precedentes, con un grado de riesgos sin precedentes, con una inseguridad sin precedentes.

Nuevos collares, el mismo perro

Los profesionales de la seguridad somos la Casandra pelma de las organizaciones, de la sociedad en su conjunto, la agorera que no hace más que anunciar los peligros mientras el resto sigue jugando en su teléfono inteligente o discutiendo cuestiones estratégicas de la compañía por Whatsapp. Y aquí estamos de nuevo advirtiendo de que seguimos usando las viejas formas de enfrentarnos a la tecnología (ignorando la seguridad por defecto en el diseño, la fabricación, despliegue, uso y mantenimiento de la tecnología) mientras los riesgos que identificamos no tienen precedente. Cuando aún nos enfrentamos con pereza al desafío del entorno SCADA industrial, un entorno imprescindible y en muchas ocasiones estratégico o crítico, aparece un hiper-conjunto de nuevas formas de aplicar sensores y conmutadores a elementos cotidianos o industriales.

Esta pereza es consecuencia del discurrir independiente de los sistemas de control industriales y de la Seguridad TIC, de primar la usabilidad y el diseño por encima de la seguridad. Nos falta diálogo fluido y nos sobra desconocimiento de los requisitos, diseño y funcionamiento. La ausencia de sensibilidad de lo que es importante para ambas partes provoca el principal problema: la falta de seguridad y privacidad en el diseño. Dos conceptos básicos aún no asimilados por todos los actores.

Y es en este momento, cuando todavía no hemos sido capaces de transmitir al entorno industrial esos dos conceptos básicos (no hablemos de las pruebas de seguridad en el proceso de fabricación, montaje y entrada en producción), cuando irrumpe el joven Internet de las cosas: a los sensores, actuadores y comunicaciones básicas o limitadas, se les añade conectividad a Internet de serie, inteligencia local, inteligencia en la nube y servicios. El Armagedón.

Riesgos y focos de atención

La inteligencia local y en la nube obligan a implementar controles en ambos espacios (el local y en la nube). Los servicios aceleran el uso y el universo IoT [Internet de las cosas], ese en el que el confort, la interrelación, la usabilidad y lo sexy están muy por encima de la seguridad. Nadie va a pagar más por evitar que su frigorífico inteligente envíe *spam* mientras le haga la compra de manera automática. Nadie es consciente de la implicación que para su vida personal y solvencia social y económica tiene que la televisión y el frigorífico nos conozca mejor que nuestra madre y no apliquen ninguna seguridad a ese conocimiento. No hay, por tanto, incentivo económico ni obligación legal para que el fabricante se plantee siquiera diseñar para una seguridad que nadie parece valorar.

Para proporcionar esos nuevos servicios, los nuevos actores –que en su inmensa mayoría no tienen una cultura TIC– deben sensibilizarse, no sólo concienciarse, de la existencia de las amenazas que pueden materializarse a través de

Nadie es consciente de la implicación que tiene para su vida que la televisión y el frigorífico nos conozca mejor que nuestra madre y no apliquen ninguna seguridad a ese conocimiento

sus dispositivos y servicios, y así aplicar controles que disminuyan el riesgo en relación con la violación de la privacidad, la seguridad de las personas, la seguridad funcional y la ciberseguridad.

El riesgo sin precedentes viene dado por la relación impacto y probabilidad que se deriva del número de dispositivos que tendremos en un futuro cercano (entre 20 y 50 mil millones de dispositivos en el 2020), la capilaridad de los mismos (llegando al cuerpo de personas y animales), la capacidad de conocer nuestra vida privada, la dependencia que generará, así como el incremento de superficie de ataque, de oportunidades de ataque y daños generados por dichos ataques.

Ya estamos viendo que los investigadores de seguridad, cuando muestran ejemplos de *hacking* sobre elementos IoT (neveras, lámparas, televisiones, instrumental médico, coches, etc.), identifican vulnerabilidades relacionadas con la gestión de la identidad, las configuraciones de caja, los modos inseguros de comunicación, etc. Así, por ejemplo, en el caso del Internet de las casas, un dispositivo, como puede ser una nevera inteligente que se conecte a nuestra agenda y correo, pone en riesgo no sólo su funcionalidad, sino también nuestros datos privados y al resto de los elementos conectados a la red residencial, con el rico y variado conjunto de información que circula por ella.

No es difícil pensar que en un porcentaje cada vez mayor de casos tendremos elementos médicos conectados a esa misma red, elementos de los que dependerán nuestras vidas y nuestra integridad física y moral. Y así ese *hacker* que ataque nuestra nevera no sólo pasará hasta la cocina, sino que se adentrará por el resto de la casa hasta llegar a los sensores y actuadores que se relacionen con nuestros cuerpos.

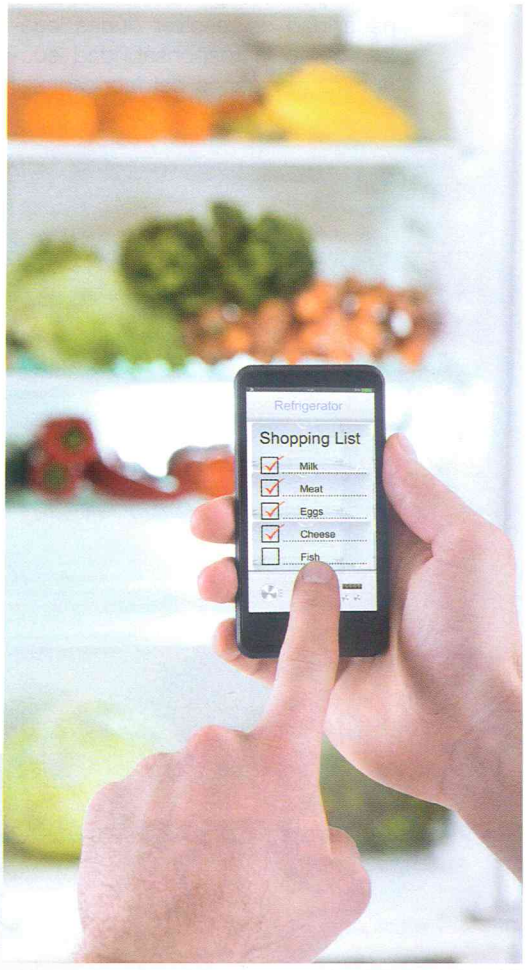
Son muchos los elementos que hemos ido apuntando para entender el porqué de esta situación: presión del negocio y falta de incentivo económico o regulatorio para invertir en seguridad; la existencia de un negocio en el petróleo del dato y el Big Data; completa ausencia de conciencia y sensibilidad por la seguridad en los usuarios y profesionales que demandan los productos; usuarios que son el producto porque no conciben pagar por servicios que cuestan dinero; y falta de madurez en el campo de la seguridad. En este capítulo vamos desde la ausencia de seguridad y privacidad en el diseño, hasta fabricantes carentes de organización de seguridad o con recursos destinados a la seguridad muy limitados, pasando por diseños orientados a la usabilidad o con fallos en la gestión de las identidades o del manejo de los protocolos de comunicación.

No vamos a mencionar el capítulo de las actualizaciones. Sólo con ver cómo se abordan por fabricantes y usuarios en los equipos finales y en los teléfonos móviles, no queremos pensar en lo que ocurrirá en el IoT, donde la consumerización no sólo será visible en el ámbito del hogar.

Datos y algunas conclusiones

Si tenemos claro que los consumidores son las mismas personas que en el ámbito laboral los denominamos profesionales, los estudios basados en encuestas arrojan unos datos preocupantes:

- La mayoría de los consumidores no están preocupados: un 64 por ciento de los encuestados está seguro de poder controlar la seguridad de sus dispositivos IoT en sus casas.
- El 65 por ciento de los consumidores tiene miedo de que sus dispositivos conectados sean hackeados, pero eso no afecta a su decisión de compra.
- Parece que los profesionales de seguridad de TI están preocupados. El 65 por ciento de ellos no se siente seguro de poder



En el Internet de las Casas, una nevera inteligente que se conecte a nuestra agenda y correo pone en riesgo no sólo su funcionalidad, sino también nuestros datos privados.

controlar esta nueva tecnología en los hogares.
- Un 88 por ciento de los expertos consultados consideran que los fabricantes no advierten a los consumidores suficientemente sobre los datos personales que recogen sus equipos.

Fuentes: HP e ISACA.

Es decir, los consumidores saben que pueden ser atacados, pero no les preocupa, los profesionales se ven desbordados y los fabricantes prefieren pasar de puntillas.

Para cambiar este desolador panorama es imprescindible sensibilizar en materia de autoprotección a los consumidores para que exijan y valoren los dispositivos seguros; definir estándares específicos para la seguridad de los mismos; obligar a las empresas que fabrican e instalan a cumplir con los estándares y a tener unos niveles de seguridad basados en la seguridad y privacidad en el diseño. En este camino no se puede dejar de contemplar la necesidad de resolver dudas legales, como la responsabilidad económica por daños del fabricante al acabar con el paradigma de producto seguro o la necesidad de obligar a las capas de gestión (incluidas las de los gobiernos) a tomarse muy en serio la magnitud del problema.

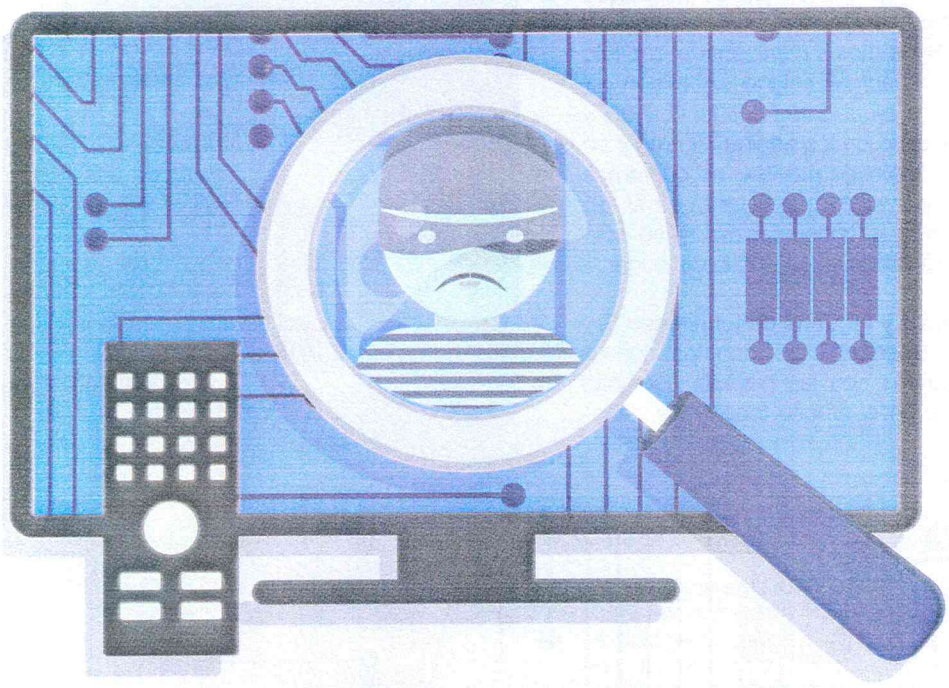
A día de hoy se han dado tímidos pasos. El 16 de septiembre de 2014, las agencias de protección de datos europeas acuñaron un dictamen de 24 páginas exclusivamente dedicado al IoT, con las siguientes conclusiones:
- que las empresas se tomen muy en serio toda la reglamentación relativa a seguridad online;
- que informen a sus usuarios de qué datos han capturado; y
- que borren la información en bruto que almacenen y se queden sólo con aquella específica del servicio que ofrecen.

> Es imprescindible sensibilizar a los consumidores para que exijan y valoren los dispositivos seguros

En el campo de la Normalización ISO hay dos proyectos en desarrollo en el JTC1/WG10 "Internet of Things"; uno es una propuesta recién iniciada sobre definiciones y vocabulario (ISO/IEC NP 2092), y el otro un AWI sobre arquitectura (ISO/IEC AWI 3014), que se inició el año pasado.

Un enfoque adecuado de la seguridad en el Internet de las cosas se basa en:
- Estándares definidos.
- Legislación adecuada a los nuevos retos (entre ellos el de la responsabilidad).
- Compromiso asumido por todas las partes intervinientes: los consumidores (residenciales y profesionales) deben adoptar entre sus necesidades la seguridad.
- Seguridad y privacidad desde el diseño, a la hora de fabricar productos y servicios.
- Comprensión y comunicación fluida entre quienes conocen la funcionalidad y los expertos de Seguridad.
- Asunción de la necesidad de protegernos ante las ciberamenazas y entendimiento del riesgo para la vida de la omnipresencia de la tecnología.

No seamos idIoTas y hagamos las cosas con seguridad.



Hace falta asumir la necesidad de protegernos ante las ciberamenazas y entender el riesgo para la vida de la omnipresencia de la tecnología.