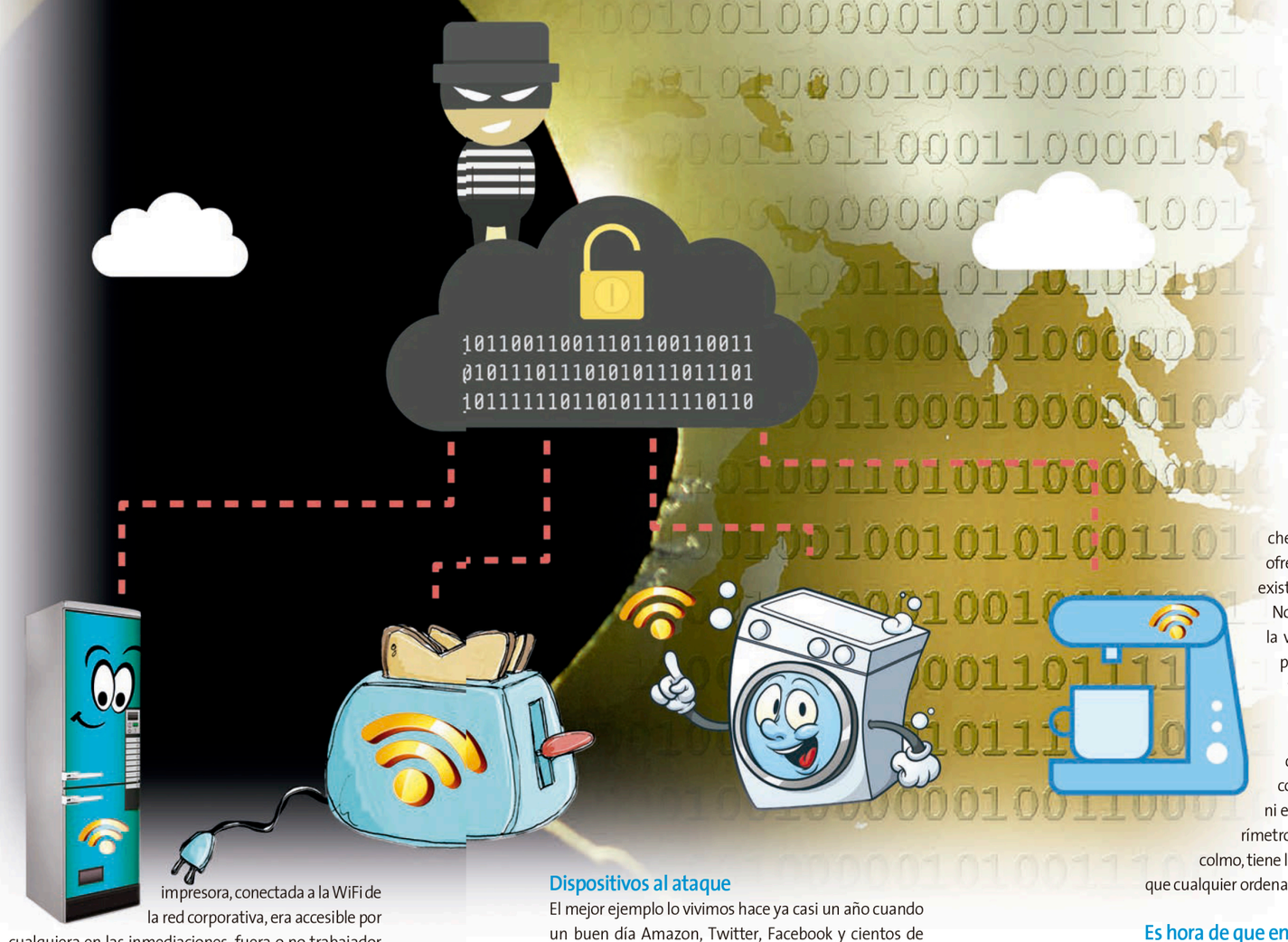
La Rebelión de "las Cosas"

¿De dónde procede ese 13,4% de pérdidas económicas en nuestra organización? De campañas de phishing a empleados de la organización. O mejor, de fugas de información, pensarás. Y bien podrías tener razón. Estos dos elementos son, junto a la seguridad de los sistemas de información de la compañía, los tres grandes detonantes del riesgo corporativo.



Pablo F. Iglesias, Analista de información en PabloYglesias.com y CTO en la consultora SocialBrains @PYDotCom

Un 13,4% anual sobre la facturación total es lo que está de media perdiendo una PYME española gracias al uso de dispositivos de IoT inseguros y no vigilados por el departamento de IT.

Pero no es el caso.

Según la encuesta realizada por Altman Vilandrie & Company en EEUU, casi la mitad (un 48%) de las empresas de este país que utilizan elementos del Internet de las Cosas dentro de su red han experimentado como mínimo alguna brecha de seguridad en los últimos años. Y el coste de dicha brecha ronda el 13,4% de los ingresos totales en compañías con ingresos menores a cinco millones de dólares, algo más de 20 millones para aquellas compañías que facturan más de 2.000 millones al año.

Es aquí donde empieza la juerga.

La encuesta se hizo a cerca de 400 directores de IT en 19 industrias distintas, y junto al dato anteriormente mencionado aparecen otros que me preocupan bastante más.

Por ejemplo, cosas tan locas como que el 68% de los encuestados consideran la seguridad del IoT como una categoría distinta. Sin embargo, solo el 43% tiene un presupuesto (y por ende, una política de actuación) independiente. O que pese a ser conscientes de que cada departamento utiliza distintos dispositivos conectados para una serie de funciones distintas, el 74% de los encuestados reconocen que las decisiones de seguridad para el Internet de las Cosas se establecen de forma centralizada.

Ahora párate un momento y piensa en la situación.

Un día cualquiera

En una organización media española. Vamos a suponer que el departamento de IT tiene relativamente bien controlada la ciberseguridad global de los activos de la compañía. Esto es: ordenadores, servidores, servicios digitales y, si eso, smartphones; lo mismo hasta impresoras, habida cuenta de que ya no es la primera compañía, ni lamentablemente será la última, que acaba en los tribunales por incumplir un contrato de confidencialidad con un cliente no porque en efecto alguien de dentro haya sacado a la luz los entresijos del mismo, sino porque la impresora, conectada a la WiFi de la red corporativa, era accesible por cualquiera en las inmediaciones, fuera o no trabajador de la misma. Pero vaya, que imaginemos este supuesto.

¿Qué pasa entonces con el resto de dispositivos que los trabajadores traen a las oficinas? Y no me refiero solo a sus smartphones personales, sino también a los relojes inteligentes, pulseras de cuantificación, auriculares bluetooth, pinchos USB, etc., etc. Dispositivos que quizás, aunque solo sea para cargar, van a enchufar en los ordenadores conectados a la red.

¿Y qué hay de todo ese Dark IT que queda fuera del perímetro de control del departamento? Ese amplificador de red que los chicos de contabilidad pusieron ya que la WiFi no llegaba bien a su zona, ese router que necesitaban los chavales de I+D para hacer pruebas sin entorpecer con sobrecarga de paquetes el resto de la red corporativa, ese aire acondicionado que tan bien nos ha venido este verano, esa cafetera/sandwichera/nevera molona que hace unos días pusieron en la sala de descanso... ¿seguimos?

La cuestión ya no es solo que el equipo IT tenga o no constancia de ello, y haya o no habilitado los controles de seguridad oportunos. La cuestión es que, de base, esta nueva oleada de dispositivos tecnológicos conectados han sido diseñados sin tener en cuenta la seguridad y privacidad de sus comunicaciones.

Dispositivos al ataque

El mejor ejemplo lo vivimos hace ya casi un año cuando un buen día Amazon, Twitter, Facebook y cientos de grandes servicios de la red estuvieron caídos durante horas por un ataque DDoS realizado no por PCs, Macs, smartphones y tablets comprometidos, sino por una botnet formada principalmente por routers y demás dispositivos del Internet de las Cosas.

Simplemente, porque mientras las organizaciones se han centrado única y exclusivamente en proteger los activos informáticos "tradicionales", toda la industria, empezando por las tecnológicas y acabando por el usuario final, han obviado hasta algo tan simple como la necesaria obligación de cambiar la contraseña por defecto de un dispositivo conectado, directa o indirectamente, a una red.

No hace mucho veíamos cómo un simple cigarrillo electrónico podía ser un vector de ataque para comprometer cualquier red corporativa. WannaCry, el ataque que sufría hace unos meses Telefónica y que ponía en jaque buena parte del resto de organizaciones mundiales, no se debió a una política laxa en los sistemas anti-phishing de los gestores de correo, ni siquiera fue debido a la poca formación en nociones básicas de seguridad que tienen la mayoría de trabajadores del siglo XXI, sino porque casi todas las redes corporativas están formadas por dispositivos que no cuentan con los parches de seguridad que el proveedor ofrece periódicamente. Estos parches existen, solo que no se llegan a aplicar. Nos está pasando ya con el IT de toda la vida, imagínate lo que nos estará pasando con el IoT, que ni siquiera va a recibir actualizaciones en todo su ciclo de vida, que viene preconfigurado para que sea solo enchufar y listo, que no pasa por los controles más básicos de seguridad ni en su diseño ni más tarde en el perímetro del departamento IT, y que para colmo, tiene la misma capacidad de hacer el mal que cualquier ordenador o smartphone.

La cuestión es que, de base, la nueva oleada de dispositivos tecnológicos conectados han sido diseñados sin tener en cuenta la seguridad y privacidad de sus comunicaciones.

Es hora de que empecemos a hablar del asunto, ¿no te parece?

¿Cuántas más personas tienen que morir de frío en Helsinki cuando en pleno invierno, con temperaturas que oscilan entre 2 y -8 ºC, un ransomware consigue secuestrar masivamente más de 230.000 termostatos "inteligentes"? ¿Cuántas más ciudades como San Francisco tienen que quedarse durante un fin de semana sin transporte público debido al hackeo del sistema de emisión de billetes para que empecemos a tomarnos en serio el asunto?

Quizás, si en vez de hablar de muertos y colapsos en ciudades, hablamos de pérdidas económicas, empezamos a tomar medidas.

Un 13,4% anual sobre la facturación total es lo que está de media perdiendo una PYME española gracias al uso de dispositivos de IoT inseguros y no vigilados por el departamento de IT. Más de 20 millones, si somos parte de una gran empresa.

Esto presuponiendo que estemos tan avanzados en cuanto a digitalización como lo están la mayoría de organizaciones en EEUU. Cosa que ya sabemos que no es verdad. Y que, de hecho, agrava el riesgo y el impacto económico del (ab)uso incontrolado de dispositivos del Internet de las Cosas. ●