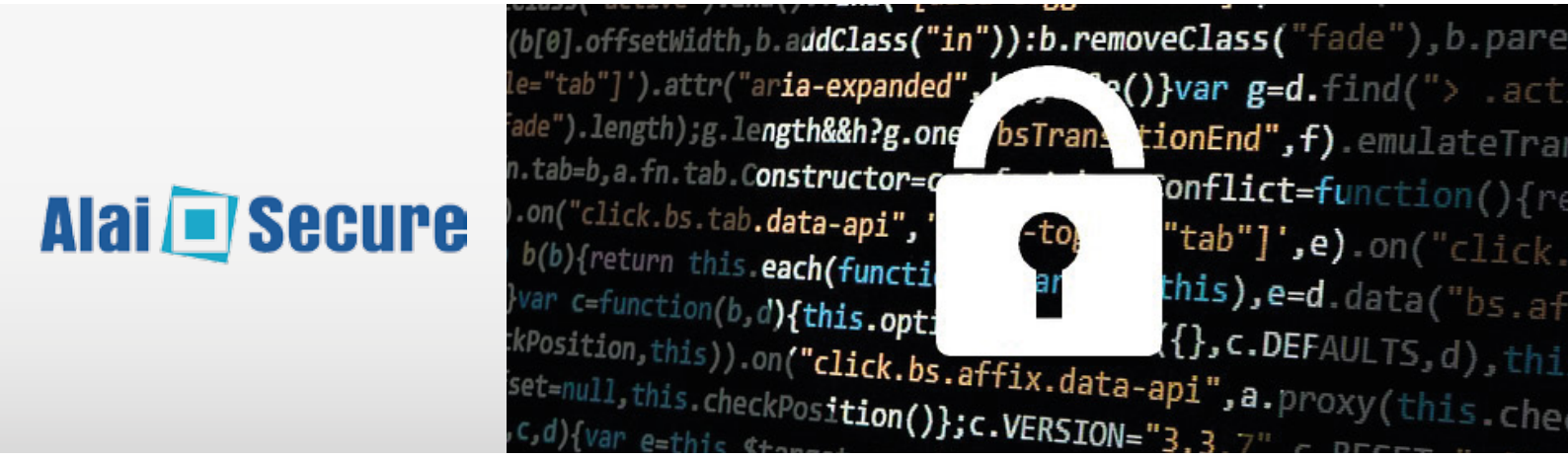
La seguridad en el IoT: “Protege lo importante porque no vas a poder proteger todo”

Security in IoT: “Protect what is important because you will not be able to protect everything”



JAVIER ANAYA | Actualmente, el término **Internet de las cosas**, IOT (Internet Of Things) se usa para definir un modelo de conexión avanzada de dispositivos, sistemas y servicios que va más allá del tradicional M2M (máquina a máquina), cubriendo una amplia variedad de protocolos de comunicaciones.

Según fuentes de la **CNMC** de hace escasamente unas semanas, hay **5,5 millones de dispositivos M2M conectados en la actualidad en España.** Este sector crece a un ritmo superior al 10% anual y se espera que alcance un volumen de unos 8 millones de conexiones en 2021. No obstante, la eclosión de la tecnología IoT está haciendo que estos números se queden pequeños. La gran cantidad de sensores, medidores, señalizaciones y demás dispositivos que se plantean a día de hoy conectados con nuestros sistemas de gestión son innumerables y hacen muy difícil la previsión de “número de conexiones” al respecto.

La aparición de **tecnologías “baratas”** que facilitan conexiones y comunicaciones está haciendo que se produzca un aluvión de empresas dedicadas a favorecer la gestión de este tipo de dispositivos. Dispositivos económicamente muy accesibles, sobre comunicaciones económicamente bajas y con tiempos de fabricación, puesta en marcha y despliegue muy bajos.

El **binomio riego-beneficio** que está presente siempre en todas las decisiones de inversión, debe cambiar inevitablemente, en este nuevo escenario donde tecnología y comunicaciones tienen un papel tan

JAVIER ANAYA | The term **Internet of Things** (IoT) is currently used to define an advanced connection model for devices, systems and services that goes beyond the traditional M2M (machine to machine), and it covers a wide range of communication protocols.

According to the **National Commission on Markets and Competition**, there are at present **5.5 million M2M devices connected in Spain**. This sector is growing more than a 10% yearly and it is expected to reach 8 million connections in 2021. However, the blooming of IoT technology is making these numbers small. The great amount of sensors, metres, indicators and other devices thought to be connected nowadays with our management systems are countless, and make very difficult to predict the number of connections.

The appearance of **“cheap” technologies** that facilitate connections and communications is generating a deluge of companies dedicated to favour the management of this kind of devices. Devices that are very accessible economically, over economically low communications and with very short production, implementation and display times.

The **pairing *risk-benefit***, which is always present in every investment decision, must change inevitably, in this new scenario where technology and communications play so important a role, for that of ***security-price.***

When deploying IoT services, **the security system associated to these devices and communications is**

importante, por el de **seguridad-precio.**

A la hora de desplegar servicios IoT **no se está teniendo en cuenta el sistema de seguridad asociado a estos dispositivos** y a estas comunicaciones. Se está dando más importancia al precio de los dispositivos y la facilidad de puesta en marcha que a su seguridad y, sí, hay muchos dispositivos, a priori, poco "atacables", poco hackeables... vamos, con muy poco interés, en acceder a ellos: La temperatura de tu frigorífico, los dispositivos de riego de tu jardín, etc.

"El binomio riego-beneficio, que está presente siempre en todas las decisiones de inversión, debe cambiar inevitablemente [...] por el de seguridad-precio"

El propio ascensor de una comunidad de vecinos parece un objetivo poco atractivo para "los malos", no obstante... **desactivar 150 ascensores y pedir un "rescate" a cambio de devolverlos a la vida** ya no parece tan "raro". La imagen de la empresa ante los clientes que les deja sin ascensor durante un tiempo, la potencial pérdida de esos clientes, aparte del propio pago de ese rescate, es decir, la propia violencia que genera un soborno de este estilo, son un problema verdadero para cualquier firma de asistencia de ascensores. Por no hablar de ascensores en instalaciones sensibles a acciones de más repercusión (centros comerciales, edificios públicos, instalaciones críticas, etc) donde **hasta el terrorismo tiene cabida.**

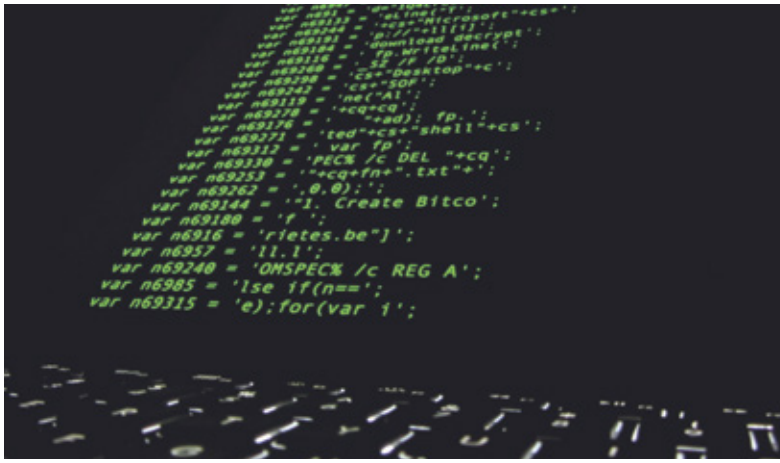
El **Ransomeware** es la técnica de cibercrimen más extendida a lo largo de todo el planeta. Sólo en España se detectaron **unos 20.000 casos en 2017**. En cuanto al **ciberterrorismo,** parece evidente que tiene un objetivo claro en este tipo de sistemas dentro de instalaciones críticas o de gran repercusión. De esta clase de ciberdelincuencia **no hay ni siquiera datos publicados**, aunque sí muchas referencias y mucha rumorología.

La propuesta de los operadores de telecomunicaciones debe ir en consonancia no sólo con el despliegue de sistemas sino también con la seguridad de esas redes. La vulnerabilidad de los sistemas se está asociando siempre a malas prácticas o falta de ellas respecto de los empleados, o a la falta de actualizaciones del sistema operativo o de los dispositivos firewall de las empresas. **Perdemos de vista, a su vez, que hay cientos de miles de rastreadores buscando por Internet dispositivos abiertos o con bajo nivel de seguridad** para ver qué pueden hacer con ellos... Recordemos el ataque que sufrieron las principales páginas web del mundo en octubre de 2016 con el ataque "MIRAI" que provocó mediante un ataque de denegación de servicio que millones de dispositivos conectados empezaran a obedecer órdenes para atacar estos sistemas.

not being taken into account. The price of the devices and the ease of its implementation are getting more importance than its security and, yes, there are a lot of devices that can be, a priori, little attackable, little "hackable", that is, of very little interest to access to them, such as the temperature of your fridge, the watering devices of your garden, etc.

"The pairing *risk-benefit*, which is always present in every investment decision, must change inevitably [...] for that of *security-price*"

The lift of a residential building seems a little appealing objective for "the bad ones". However, **disabling 150 lifts and asking for a ransom to reactivate them** does not seem so strange. The company's image with regard to clients left with no service for some time, the possible loss of those clients, apart from the payment of the ransom, that is, the violence generated by this kind of bribery, are a real problem for any lift assistance company. Not to mention lifts in buildings sensitive to actions with bigger consequences (shopping centres, government buildings, critical facilities, etc) where **there is place even for terrorism.**



Ransomware is the most widespread cybercrime technique in the world. **20,000 cases were detected in 2017** only in Spain. Regarding **cyberterrorism**, it seems obvious that it has a clear objective in this kind of systems inside critical facilities or those having great impact. **There is no published data** about this type of cyberdelinquency, but there are many references and rumours.

The proposal of telecommunications operators must go in line with the systems deployment but also with the security of those networks. The systems vulnerability is being always associated to bad practices or the lack of these ones by the employees, or to not updating the operating systems or the firewalls of the companies. **At the same time we overlook the fact that there are hundreds of thousands of trackers searching the**

Cuando una empresa de fabricación de cartón ve secuestrados sus ordenadores, su servidor y, por consiguiente, sus datos, no podían creerse objetivo de nadie y sin embargo se veía obligada a pagar **10.000 euros en menos de 12 horas** para poder recuperar "su vida". Un solo dispositivo remoto conectado a un proceso de fabricación mediante una **"cheap network"** facilitó la entrada a su sistema de gestión de alarmas y a su sistema de gestión. A partir de ahí, el resto fue muy sencillo. Estos cientos de miles de rastreadores encuentran puertas abiertas a través de dispositivos conectados a internet sin la suficiente seguridad y **no sólo porque los empleados no cumplan las normas o los sistemas no se actualicen adecuadamente.**

Los operadores somos responsables de que todos los dispositivos estén, **no sólo conectados y facilitando despliegues, sino conectados con la suficiente seguridad.** El sistema GPRS/GSM lleva 25 años demostrando que es el sistema que más seguridad ofrece y por ello debe ser prioritario en función de la seguridad requerida. El resto de comunicaciones: cheap network, banda libre, etc, por supuesto, son operativas, **pero no para comunicaciones que requieran un cierto nivel de seguridad.**

"El Ransomeware es la técnica de cibercrimen más extendida a lo largo de todo el planeta"

Algunos operadores de telecomunicaciones no tiramos la toalla y seguimos pensando en **fórmulas para evitar y contrarrestar este tipo de ataques:** securizando las comunicaciones -a través de VPN- entre el ascensor y la central, y entre el ascensor y el técnico de mantenimiento desplazado, garantizando el 0% de hiperactividad, protegiendo las comunicaciones frente a ataques de denegación de servicio, controlando y gestionando los enrutamientos de las direcciones IP, etc. **Todas las medidas son pocas**. Debemos exigirle a nuestro Operador de Telecomunicaciones que nos ofrezca siempre el mayor nivel de seguridad en cada momento para garantizar la Seguridad de nuestras comunicaciones. Ya sea para proteger un automóvil en movimiento como un ascensor de una comunidad de vecinos sencilla.

A finales de 2015 se reunió un panel de expertos relacionados con la Sociedad de la Información, Ingenieros, empresarios, Fuerzas de Seguridad, institutos de Seguridad informática de varios países, catedráticos universitarios, sociólogos, políticos, etc, se dieron cita para hablar de seguridad. Los resultados se presentaron en un informe bajo un título que resumía todas las conclusiones en una: **"Protege lo importante, porque no vas a poder proteger todo..."**

Internet for open devices or devices with a low level of security to see what they can do with them. We must remember the attack suffered by the world's main web pages in October 2016 with "MIRAI" that caused, by way of a denial-of-service attack, millions of connected devices to start taking orders to attack these systems.

When a company that produces cardboards has its computers and server and, as a result, also its data hijacked, it could not believe to be the objective of anybody. Nevertheless, it was forced to pay **10,000 euros in less than 12 hours** to recover its "life". One single device remotely connected to a production process through **a cheap network** facilitated the entrance to its alarm and management systems. From there, the rest was very simple. These hundreds of thousands of trackers find open doors through devices connected to the Internet without the sufficient security and **not only because the employees do not comply with the rules or because the systems are not adequately updated.**

The operators are responsible of getting all the devices **connected and facilitating deployment, especially of having them connected with sufficient** security. The GPRS/GSM system has been 25 years demonstrating it is the system that offers the greatest security and thus it must be preferential based on the required security. The rest of communications (cheap network, unlicensed band, etc) are operational, of course, **but not for communications that require certain security level.**

"Ransomware is the most widespread cybercrime technique in the world"

Some telecoms operators do not throw in the towel and we keep thinking of **methods to avoid and counteract this kind of attacks**: by making communications secure –through VPN- between the lift and the head office, and between the lift and the maintenance technician; ensuring a 0% hyperactivity; protecting communications against denial-of-service attacks; controlling and managing the routing of IP addresses, etc. **All possible measures are too few**. We must demand our telecommunications operator to always offer us the highest security level at every moment to ensure the security of our communications. Be it for protecting a moving car or an easy building lift.

At the end of 2015 a board of experts related to information society met. Engineers, businessmen, security forces, computer security institutes from different countries, university professors, sociologists, politicians... met up to talk about security. The results were presented in a report under a title that summarized all the conclusions in one: **"Protect what is important because you will not be able to protect everything".**