SMART TECHNOLOGY TOPICS

Ciberseguridad

19 de Mayo de 2021

Organizan:

KNX NATIONAL ESPAÑA

SMARTECH CLUSTER

SMART TECHNOLOGY TOPICS

Principios básicos de la Ciberseguridad

19 de Mayo de 2021

Sergio Hernández
Presidente Smartech Cluster

Organizan:

KNX NATIONAL ESPAÑA

SMARTECH CLUSTER

SMARTECH CLUSTER

Índice

¿Qué es la Ciberseguridad?

Definición formal:

La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

Categorías

- La **seguridad de red**
- La **seguridad de las aplicaciones**
- La **seguridad de la información**
- La **seguridad operativa**
- La **recuperación ante desastres y la continuidad del negocio**
- La **capacitación del usuario final**

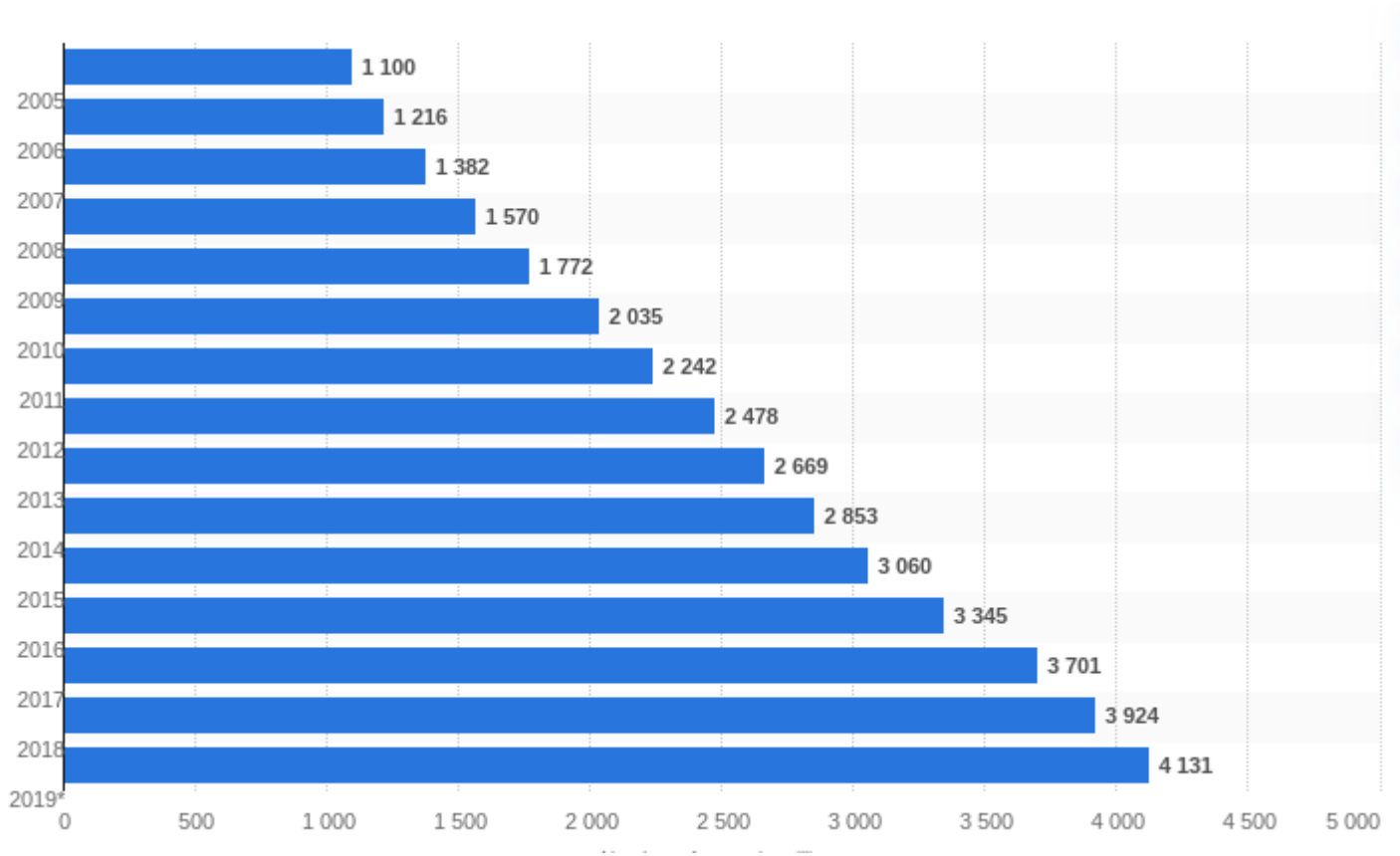
¿Por qué la Ciberseguridad?

Razones:

- **Preservar los datos.**
- **Proteger datos ante manipulaciones.**
- **Proteger el acceso a ellos.**
- **Proteger la operatividad de sistemas y su integridad.**
- **Evitar la instalación de espías o roben (datos, sonidos e imágenes).**
- **Evitar caballos de troya**, o la activación de puertas traseras, que permitan tomar el control de nuestros sistemas.
- **Protección de dispositivos personales** (portátiles, móviles) ante pérdidas y robos.

¿Por qué ahora es tan importante?

Veamos unos números



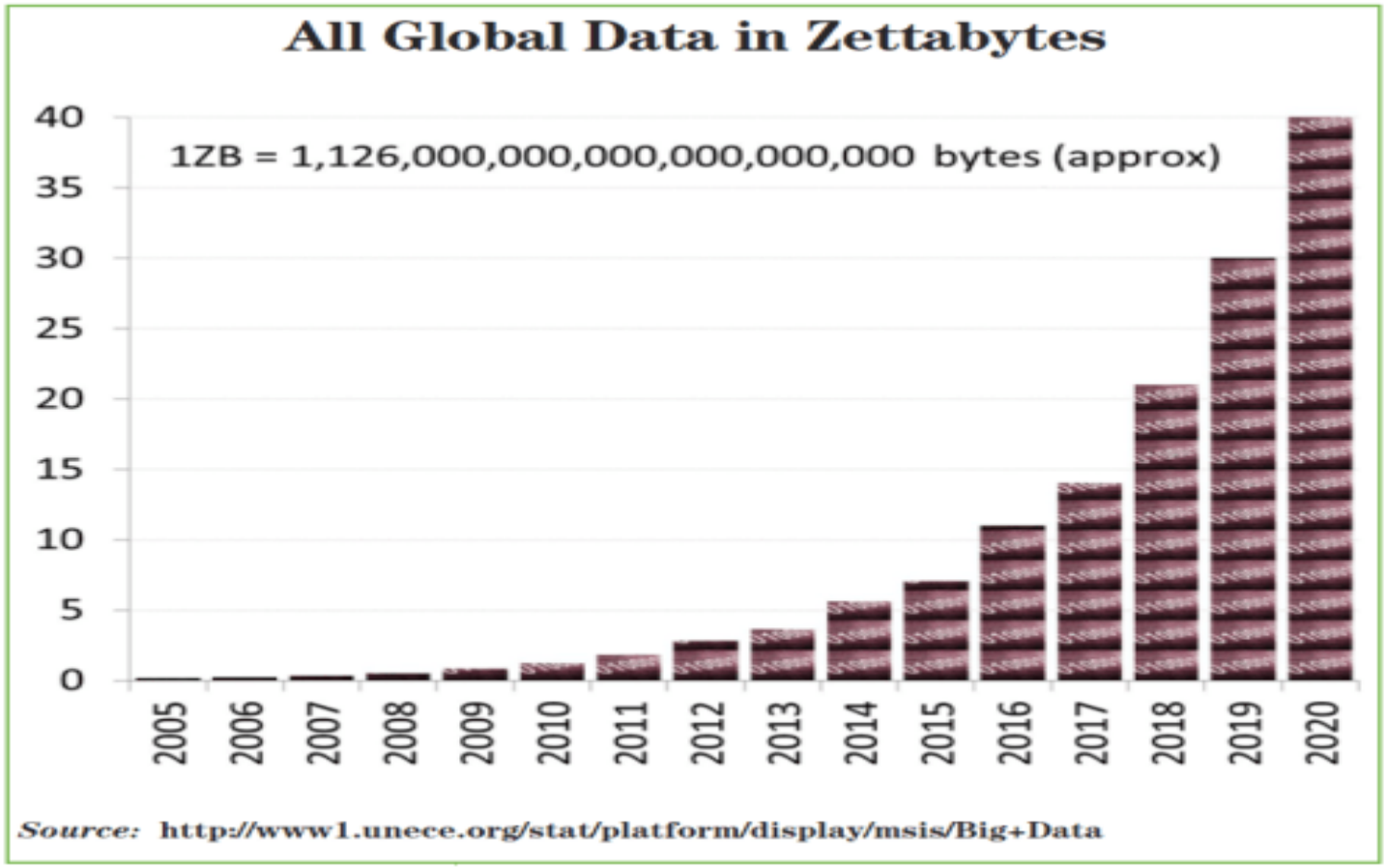
Crecimiento Internet:

Población mundial: 7.700 Mio personas

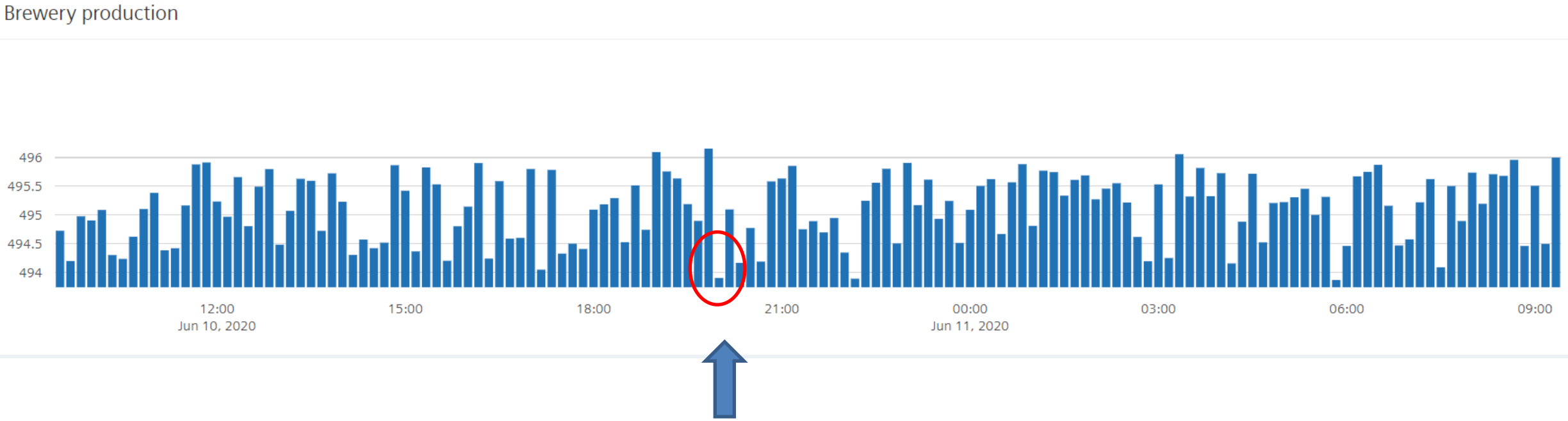
Usuarios Internet: 4.100 Mio personas

53% de usuarios conectados.

Veamos más números



¿Y para que sirven tantos datos?



¿Qué ha pasado aquí?

La importancia de los datos

- Anteriormente, muestras cada 15 minutos, como hemos observado en la gráfica anterior.
- Gracias al BIG DATA pasamos de un muestreo discreto a un muestre en tiempo real, lo que implica.
- Necesidad de más servidores, entes de AI para procesarlos y por tanto, sistemas de Ciberseguridad para protegerlos

→ CRECIMIENTO EXPONENCIAL

¿De quien depende la Ciberseguridad?

Pero hablando de instalaciones ….

Seguridad de productos y soluciones (PSS)

Productos:

Protección de clientes y productos contra daños causados (directa o indirectamente) por la insuficiente capacidad de recuperación de los productos, soluciones o servicios contra el acceso, cambio o destrucción no autorizados.

Seguridad de la información

Tecnología Información (IT)	**Tecnología Operacional (OT)**
La seguridad IT es el aspecto de la información de la seguridad focalizado en la protección de la información de los activos, si estos son procesados en forma de datos. El objetivo es asegurar el correcto uso de la tecnología para proteger los datos, según requerimientos.	OT es hardware y software que detecta o causa un cambio a través de la visualización y/o control de un dispositivo físico, proceso o evento de una empresa. Esto incluye todo tipo de infraestructuras gestionadas y redes especiales.)


*WARE
software
hardware
ransomware

¿Cómo debemos proteger nuestra instalación?

En primer lugar veamos 6 vías de evitar Ciberataques:

- **Evaluación técnica.** "Hay que saber en qué estado se encuentra la instalación. Así se puede establecer las medidas específicas". Esto implica realizar auditorías técnicas e implantar soluciones de seguridad en la nube. También es necesario exigir certificados de confianza digital a clientes y proveedores. Tampoco hay que olvidarse de implantar altos niveles de ciberseguridad en los sistemas SCADA (Supervisión, Control y Adquisición de Datos).

- **Monitorizar los sistemas de seguridad de la información.** Hay que proteger las redes industriales (equipos o maquinaria que operan conectados a internet) y a las redes corporativas (como los ordenadores de los empleados).

- **Cuidado con los servidores web.** Precaución con los servidores web para configurar los dispositivos industriales ya que estos servidores se pueden convertir en un vector de ataque.

¿Cómo debemos proteger nuestra instalación?

En primer lugar veamos 6 vías de evitar Ciberataques:

- **Especial atención a Internet de las Cosas.** Los riesgos están relacionados con la convergencia de múltiples plataformas y aplicaciones en sistemas embebidos. Por ejemplo, en el caso de los edificios inteligentes se emplean sistemas conectados para medir aspectos como la climatización o hacer un uso eficiente de la energía que, de nuevo, abren la puerta a los atacantes.

- **Intercambio de información.** "Hace falta un sistema ágil de intercambio de información sobre los ataques en tiempo real", sería idóneo establecer un método actualizado de gestión de riesgos, ya que "así se fomentaría una defensa proactiva frente a la reactiva que es la que se asume hoy".

- **Concienciación de los empleados.** Un ciberataque puede llegar desde cualquier parte y a veces son los propios empleados los que permiten la entrada de los hackers. De hecho, uno de los métodos favoritos de los ciberdelincuentes es enviar un correo con un archivo infectado para que se lo descarguen los trabajadores y así poder acceder a los sistemas internos.

Recomendaciones

- Utilizar siempre sistemas que dispongan de todas las garantías a nivel de Ciberseguridad: Exigir la documentación y certificados correspondientes.

Esto es válido tanto para:

- Canal profesional: Ofrecer soluciones a su cliente final de total garantia, exigiendo al proveedor los mismos.

- Usuario final: Explicarle sus derechos y aclarar sus miedos sobre la Ciberseguridad.

Casos de ataques de Ciberseguridad

DELITOS ABRIL 27 DE 2020

Judicializan a ciudadano por presuntos robos a cuentas bancarias

NOVEDADES TECNOLOGÍA ABRIL 17 DE 2020

Gmail bloquea correos maliciosos relacionados con covid-19

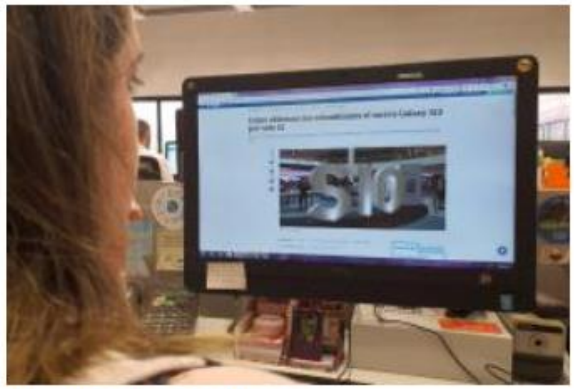
NOVEDADES TECNOLOGÍA MARZO 28 DE 2020

15 consejos de ciberseguridad para no exponerse en la red

NOVEDADES TECNOLOGÍA MARZO 25 DE 2020

El teletrabajo puede abrir puertas a ciberataques

Casos de ataques de Ciberseguridad



NOVEDADES TECNOLOGÍA FEBRERO 25 DE 2020

Recomendaciones para evitar engaños y estafas mientras usa internet

NOVEDADES TECNOLOGÍA FEBRERO 17 DE 2020

'Utilizó un rostro falso y me desangró': mujer estafada en Internet

NOVEDADES TECNOLOGÍA FEBRERO 01 DE 2020

Las ciberamenazas de las que más debe cuidarse este año

TUTORIALES TECNOLOGÍA
DICIEMBRE 16 DE 2019

Viajes gratis, fincas que no existen y otros ciberengaños de temporada

Casos de ataques de Ciberseguridad

APPS NOVIEMBRE 20 DE 2019

Videos MP4 exponen datos personales de usuarios en WhatsApp

NOVEDADES TECNOLOGÍA OCTUBRE 29 DE 2019

2.4 millones de datos de colombianos fueron expuestos en la red

NOVEDADES TECNOLOGÍA AGOSTO 15 DE 2019

Secuestrar sus datos es cada vez más fácil

BARRANQUILLA JULIO 25 DE 2019

Millonario robo de 'hackers' a funcionarios judiciales de Barranquilla

En resumen

SMART TECHNOLOGY TOPICS

Máxima ciberseguridad mediante KNX SECURE

19 de Mayo de 2021

Michael Sartor
Asociación KNX España
Secretario Técnico

Organizan:

KNX NATIONAL ESPAÑA

SMARTECH CLUSTER

KNX NATIONAL ESPAÑA

Índice

Noticias aparecidas en diferentes medios de comunicación

Home > Security

Smart home hacking is easier than you think

RELATED

How to keep your connected home safe: 7 steps you can take to boost home...

What can I do with home automation?

What is home automation and how do I get started?

on IDG Answers

Why is my Belkin range extender not

Scary stories of hackin
emerging, but how real

By Colin Neagle | Follow
Network World | Apr 2, 201

RELATED TOPICS
Security
Internet of Things

Last Marc
review on
home – re

BUSINESS INSIDER UK

TECH

Smart home devices could put you in danger

Cadie Thompson

Jul. 15, 2015, 11:39 PM 289

FACEBOOK LINKEDIN TWITTER EMAIL

Smart home products are supposed to help keep you safe, but some of these connected devices could put you in danger.

As home automation products flood the market, there's growing concern that these internet connected devices — like smart cameras and thermostats — are an easy target for hackers because they lack basic security measures.

"Really, the state of security on these things right now is pretty atrocious," Colby Moore, a security research engineer at the cybersecurity firm Synack, told Business Insider.

Stocksnapper/Shutterstock

Poor security on smart home devices can enable hackers to know when you aren't at home.

How Hackers Violate Privacy and Security of the Smart Home

POSTED IN HACKING ON SEPTEMBER 11, 2015

SHARE

The Technology Invade

The rapid growth of the paradigm of the
significant way our concept of "house."
new generation of smart appliances pro
comfortable, but we cannot underestim

The solutions for home automation are
majority of cases lack security: security e
meters are an easy target for hackers.

INTERNET

Un 'hacker' español piratea un hotel de lu China

Jesús Molina, que trabaja como asesor independiente en San Francisco, asegura que pudo hacerlo porque el estándar de domótica que utilizaba el establecimiento fue diseñado en los 90

MICHAEL MCLOUGHLIN | MADRID
@MICHAELMCSAEZ
3 agosto 2014
16:05

El hotel 'hackeado', St. regis en Shezhen, en Hong Kong. / Hotel St Regis

Que si un agujero en Whatsapp, que si una brecha en los sistemas de Facebook, que si han conseguido eludir los sistemas de bloqueo del iPhone... Cada cierto tiempo, salta la noticia de que algún experto informátic a los responsables de seguridad de alguna que otra empresa de internet tras andar escrutando las entrañas de

Unas de las últimas muescas que se han grabado en este palmarés de 'hackers' es la de un analista español Ciudad Real. Jesús Molina, que reside en Estados Unidos desde hace una década, ha conseguido piratear el sistema por el que se controlan las habitaciones de un hotel chino. Y no en cualquier local, si no en un cinco estrellas como St. Regis de Shénzhen, una urbe cercana a la cosmopolita Hong-Kong.

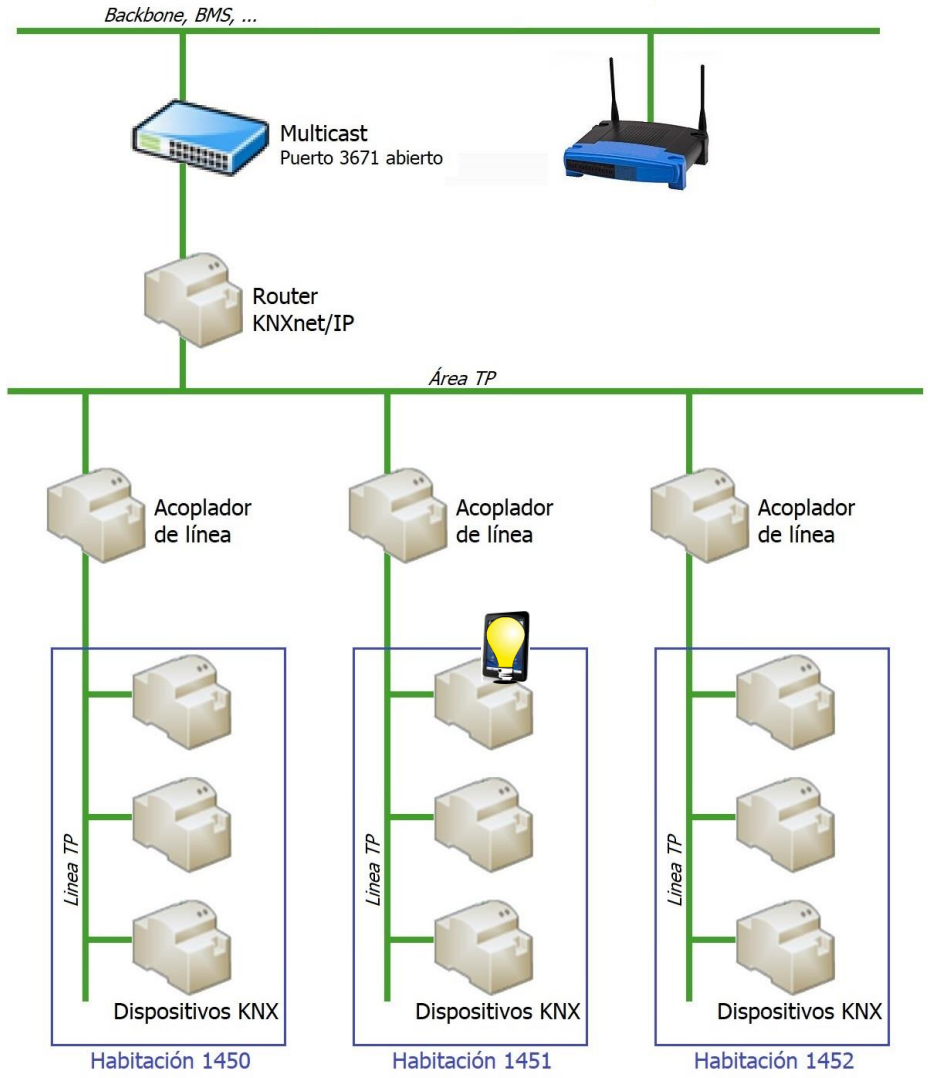
KIM ZETTER SECURITY 07.17.14 6:30 AM

HERE'S HOW EASY IT COULD BE FOR HACKERS TO CONTROL YOUR HOTEL ROOM

A view of the St. Regis Shenzhen hotel. St. Regis

SHENZHEN IS THE Silicon Valley of mainland China. Situated about 50 minutes north of Hong Kong, the modern city is home to the Shenzhen Stock Exchange and numerous high-

Escenarios reales de pirateo informático
Ejemplo 1: Hotel



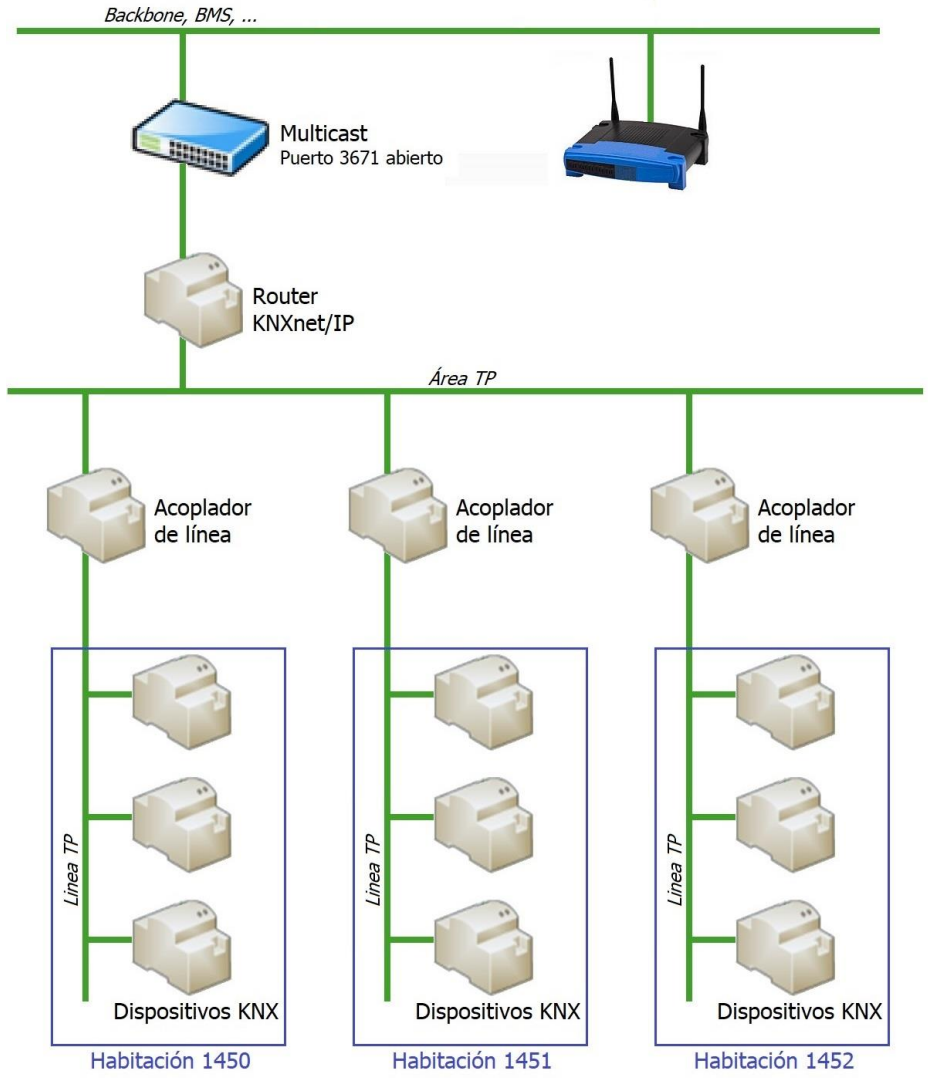
Situación:

- Dispositivos KNX controlan varias funciones (iluminación, climatización, persianas, etc.) en cada habitación de un hotel. A través de una línea principal (p.ej. BMS) se controlan todas las habitaciones.
- El cliente ocupa la habitación 1451 y recibe una tablet para controlar las funciones dentro de su habitación (“Butler-App”).

  Ejemplo: el cliente enciende la luz desde su tablet .
- El cliente recibe también una contraseña WiFi para acceder con su portátil a internet.

- **Hasta ahí – todo bien.**

Escenarios reales de pirateo informático
Ejemplo 1: Hotel

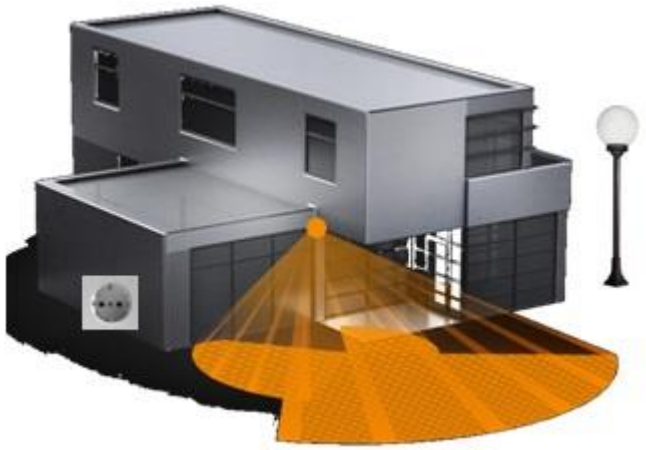


Pirateo informático:

- Es evidente que la tablet de su habitación usa una conexión WiFi para controlar las funciones.
- El hacker, con amplios conocimientos informáticos y también de la herramienta ETS, usa su portátil y la conexión a internet para detectar que se usa el puerto abierto 3671.
- La conexión WiFi de la tablet está aparentemente protegida, pero el hacker intenta abrirla usando la contraseña que ha recibido para conectarse a internet. ¡Y da resultado!
- El hacker pide una nueva habitación, cerca de la anterior, y desde ahí puede controlar las funciones de la habitación anterior usando la contraseña de esa habitación.

  Ejemplo: el hacker enciende la luz desde su portátil.

Escenarios reales de pirateo informático
Ejemplo 2: Vivienda



Situación:

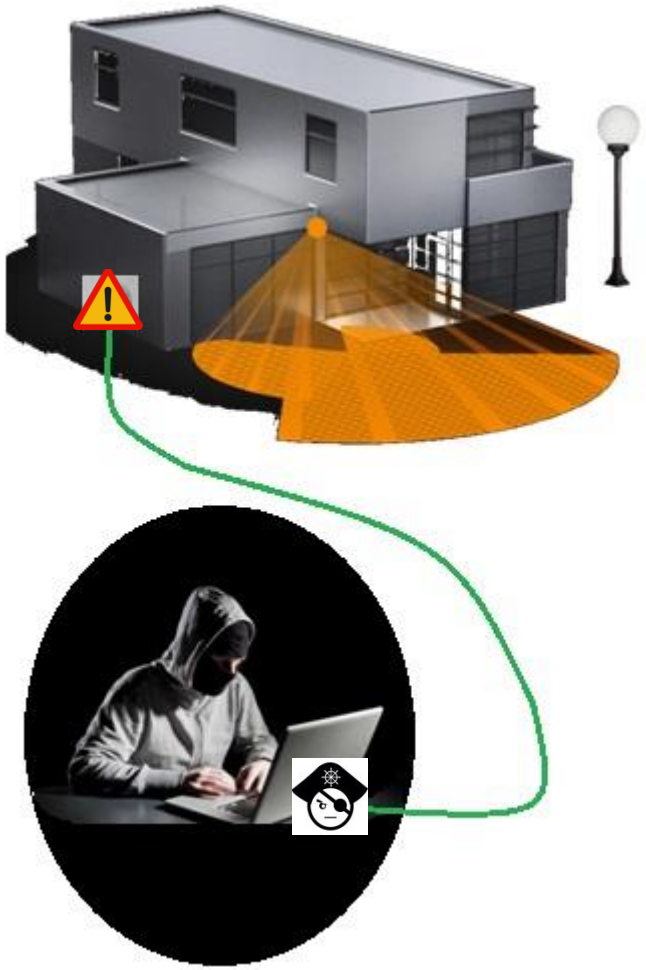
- En una vivienda unifamiliar, KNX controla todas las funciones dentro de la vivienda: iluminación, climatización, persianas/toldos, alarmas, etc.

- KNX controla también varias funciones en el exterior de la vivienda, como p.ej. el alumbrado, un detector de movimientos, una toma de corriente, etc.

- **Hasta ahí – todo bien.**

Escenarios reales de pirateo informático

Ejemplo 2: Vivienda



Pirateo informático:

- Los dispositivos KNX exteriores no se han protegido adecuadamente para impedir el acceso físico al bus de comunicación.
- El hacker desmonta la toma de corriente y tiene acceso al bus KNX.
- Con las herramientas informáticas y los conocimientos necesarios puede tomar control sobre toda la instalación, modificar parámetros, leer datos (p.ej. código de acceso), etc.

Escenarios reales de pirateo informático

¿Se podrían haber evitado estos casos?

¡Por supuesto que sí!

Teniendo en cuenta las medidas recomendadas por KNX para proteger una instalación.

KNX recomienda estas tres medidas de ciberseguridad

Medidas simples para impedir el acceso al bus de comunicación

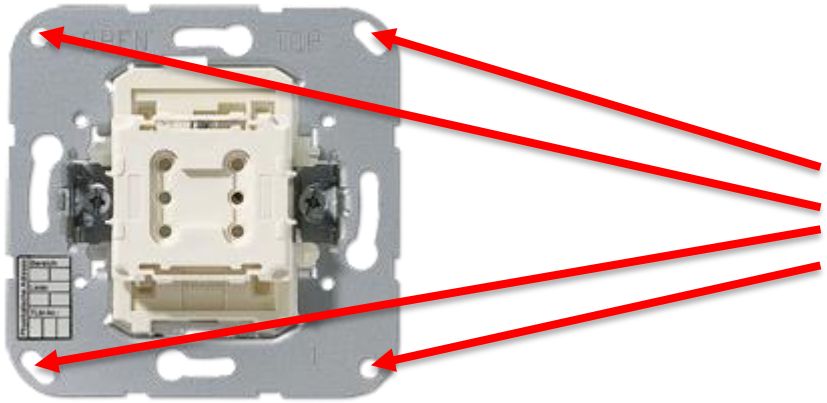
Medidas mediante configuración / programación

KNX Data Secure / KNX IP Secure

Medidas de ciberseguridad

Medidas simples para impedir el acceso al bus de comunicación

Los dispositivos deben ser fijados adecuadamente para evitar que se puedan desmontar de forma fácil.



Atornille todos los dispositivos de forma segura, usando por ejemplo tornillos y tuercas antirrobo que pueden ser removidos sólo con herramientas especiales.

Medidas de ciberseguridad

Medidas simples para impedir el acceso al bus de comunicación

Los cuadros eléctricos equipados con dispositivos KNX deben estar cerrados con llave, y/o ubicados en espacios con acceso restringido.

Instale el cuadro eléctrico en sitios con acceso sólo para personas autorizadas

Cierre y bloquee con llave la puerta del cuadro eléctrico

Si no puede ubicar los cuadros eléctricos en espacios con acceso restringido, use dos cuadros independientes.

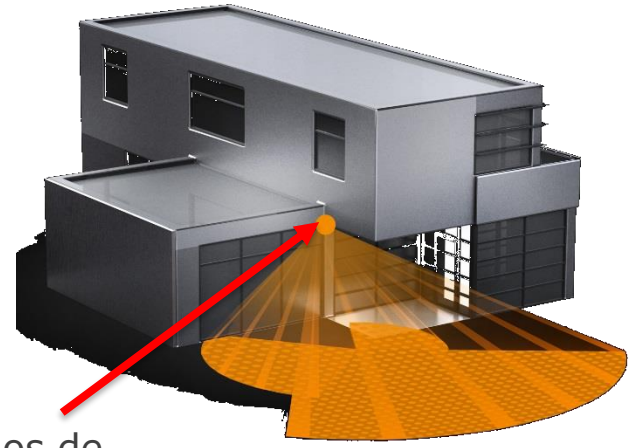
Cuadro eléctrico con elementos accesibles a todo el público, por ejemplo magnetotérmicos

Cuadro eléctrico con dispositivos KNX y otros elementos de seguridad, cerrado con llave

Medidas de ciberseguridad

Medidas simples para impedir el acceso al bus de comunicación

Los dispositivos instalados en el exterior (sensores de movimiento, estaciones meteorológicas, cámaras de video-vigilancia, etc.) son una puerta de entrada preferida para hackers.

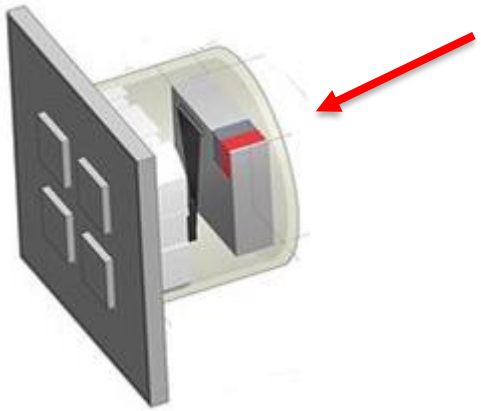


Ubique los dispositivos en sitios de difícil acceso (p.ej. a gran altura), y protéjalos adecuadamente

Medidas de ciberseguridad

Medidas simples para impedir el acceso al bus de comunicación

En caso necesario, como alternativa a los dispositivos con BCU incorporada puede usar dispositivos convencionales conectados a entradas binarias instaladas en espacios de difícil acceso.



Dispositivos con la BCU incorporada permiten un acceso directo al bus KNX

Entradas binarias permiten el uso de dispositivos convencionales y evitan el acceso al bus

KNX recomienda estas tres medidas de ciberseguridad

Medidas simples para impedir el acceso al bus de comunicación

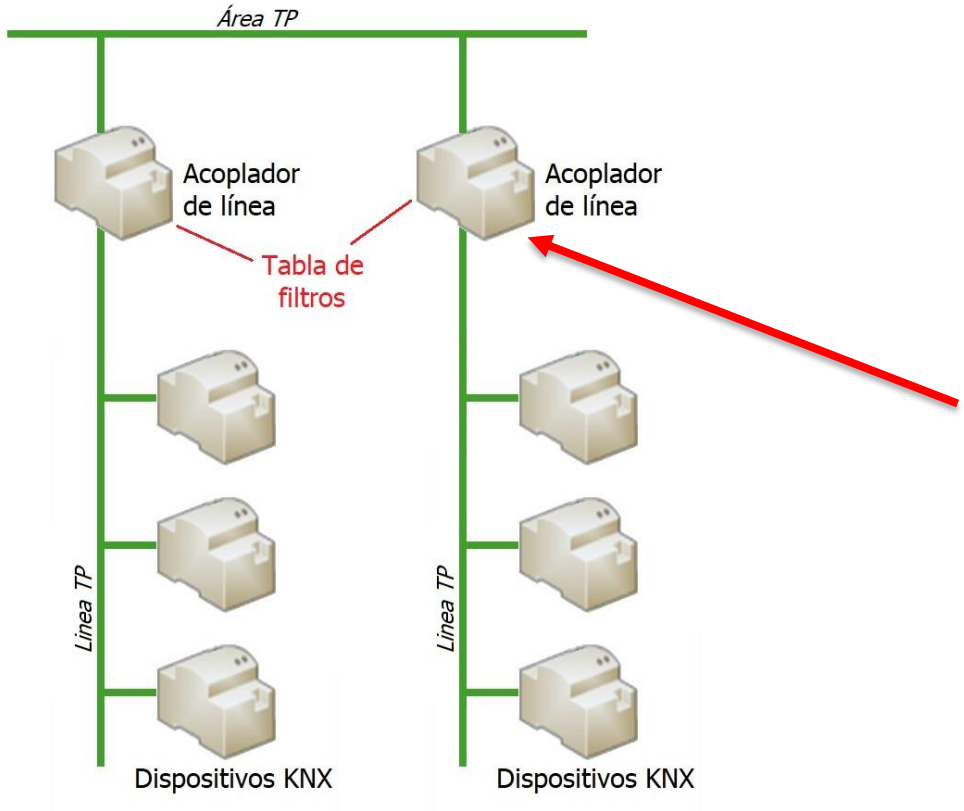
Medidas mediante configuración / programación

KNX Data Secure / KNX IP Secure

Medidas de ciberseguridad
Medidas mediante configuración / programación

Par Trenzado (Twisted Pair, TP):

Para dispositivos instalados en áreas de poca vigilancia (exterior, parkings, lavabos, almacén, etc.) se puede prever una línea independiente



Las tablas de filtro en los acopladores de línea evitan que un hacker tenga acceso a toda la instalación

Medidas de ciberseguridad
Medidas mediante configuración / programación

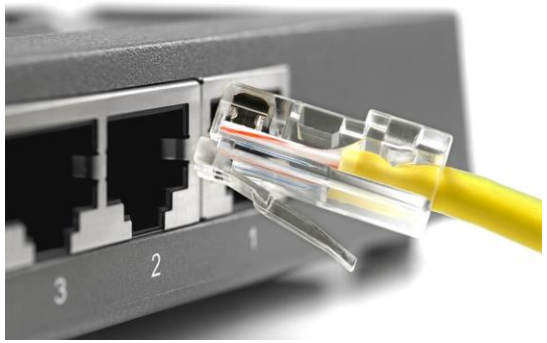
Línea de fuerza (Power Line, PL):

Se recomienda el uso de filtros electrónicos para filtrar las señales entrantes y salientes

Con el uso de filtros electrónicos, los telegramas se limitan a una única línea

Medidas de ciberseguridad
Medidas mediante configuración / programación

Comunicación IP cableada (p.ej. Ethernet) / inalámbrica (p.ej. WiFi):
Sistemas de automatización de edificios deberían usar una red independiente con su propio hardware (acopladores, enrutadores, …).



Use los mecanismos de protección conocidos para redes IP:

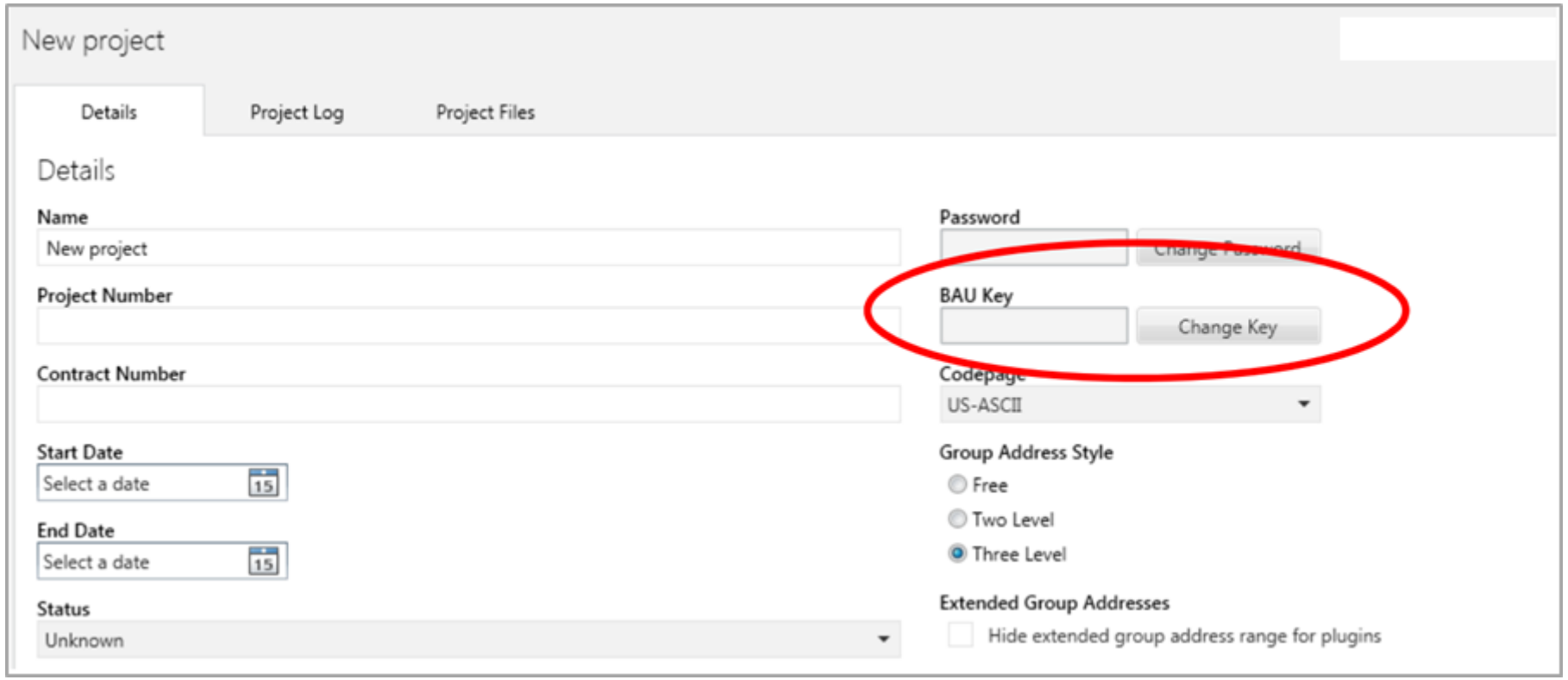
- Filtros MAC
- Encriptación del WLAN (WPA2)
- Cambiar y ocultar SSID
- La instalación LAN o WLAN debería estar protegida mediante firewalls.
- En caso de que no sea necesario un acceso externo a la instalación, la puerta de enlace predeterminada se puede establecer en 0, bloqueando así cualquier comunicación a internet.
- Asegure que el acceso a la instalación KNX sea a través de conexiones VPN (requiere enrutador o servidor con funcionalidad VPN).
- Use soluciones dedicadas de fabricantes específicos (por ejemplo, aquellos que permiten un acceso https).

Medidas de ciberseguridad

Medidas mediante configuración / programación

Protección mediante configuración ETS:

ETS permite definir contraseñas de bloqueo para cada proyecto.
Esta configuración no puede ser leída / modificada por personas no autorizadas



Medidas de ciberseguridad

Medidas mediante configuración / programación

Pero sobre todo:

¡¡¡No invente la rueda!!!

Para proyectos de gran envergadura, no dude en involucrar especialistas en integración de sistemas, incluso de tecnologías IT, para medidas de ciberseguridad adicionales.

KNX recomienda estas tres medidas de ciberseguridad

Medidas simples para impedir el acceso al bus de comunicación

Medidas mediante configuración / programación

KNX Data Secure / KNX IP Secure

Antes de conocer los detalles…….. ¿qué es AES?

Advanced Encryption Standard (AES):

Se trata de un estándar internacional que describe un algoritmo de encriptación (ISO/IEC 18033-3)

EN KNX Secure usamos el AES-128

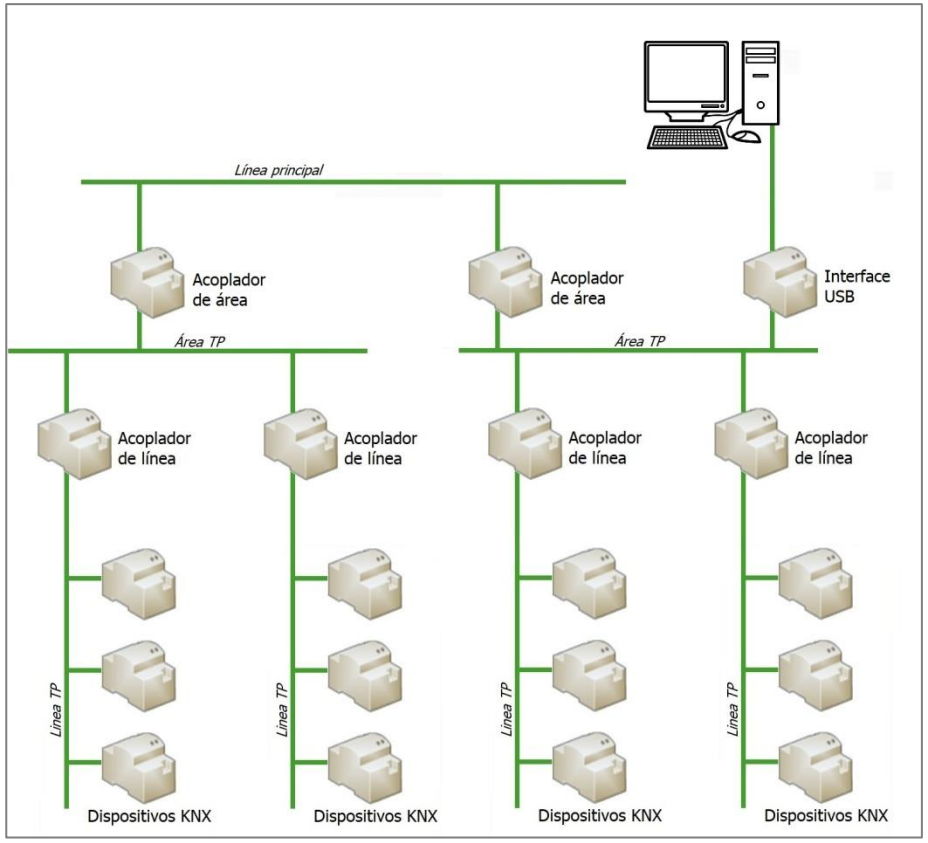
Métodos de encriptación:

- **Clave de 128 bit**
- **Sustitución de bytes**
- **Cambio de filas**
- **Mezcla de columnas**
- **AddRoundKey**

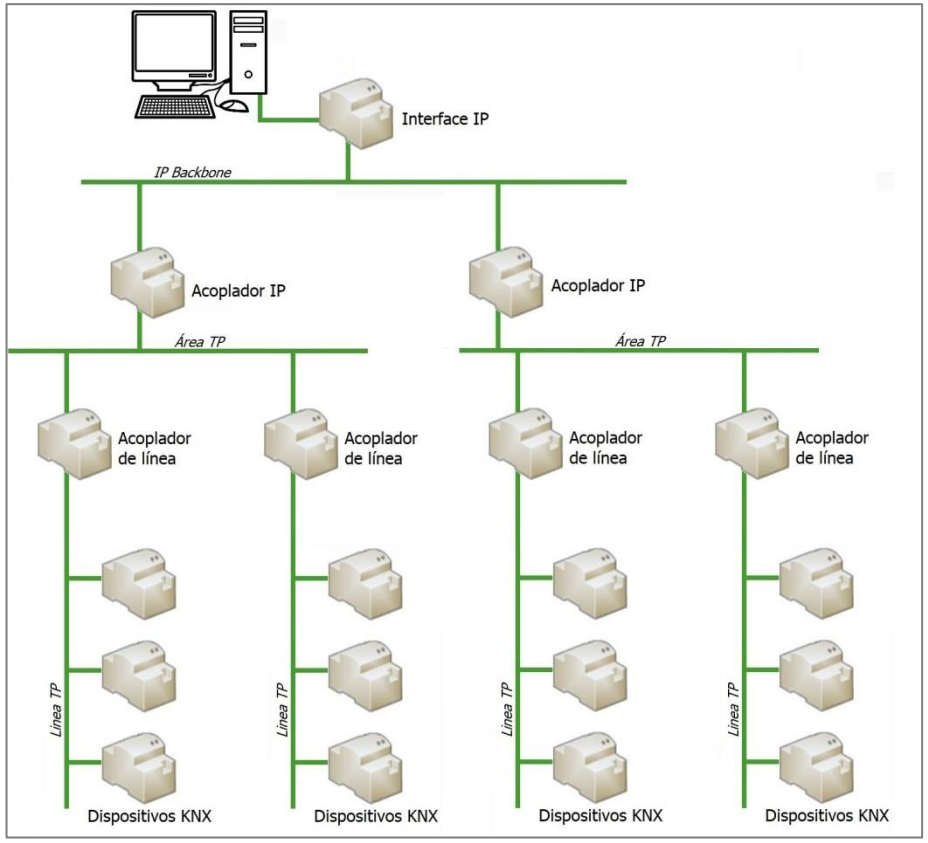
Medidas de ciberseguridad
KNX Data Secure / KNX IP Secure

KNX ha desarrollado un doble concepto de protección:

KNX Data Secure, para la transmisión segura de telegramas dentro de una instalación KNX



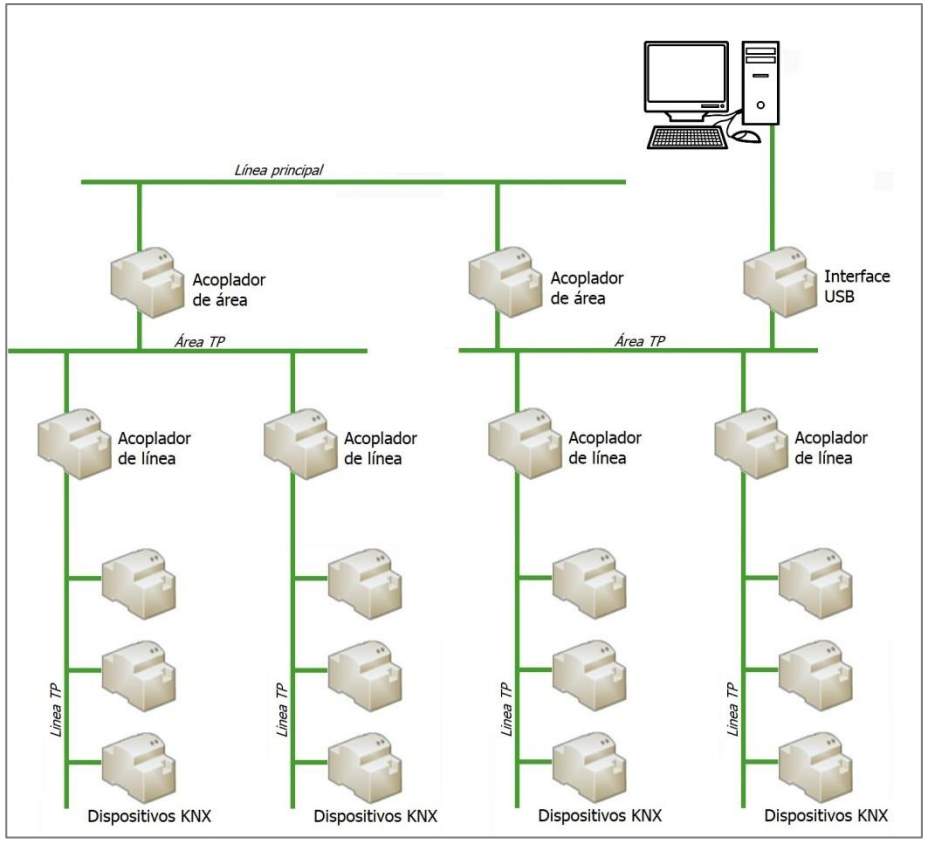
KNX IP Secure, para la transmisión segura vía IP



Medidas de ciberseguridad
KNX Data Secure / KNX IP Secure

KNX Data Secure

Para la transmisión segura de telegramas dentro de una instalación KNX



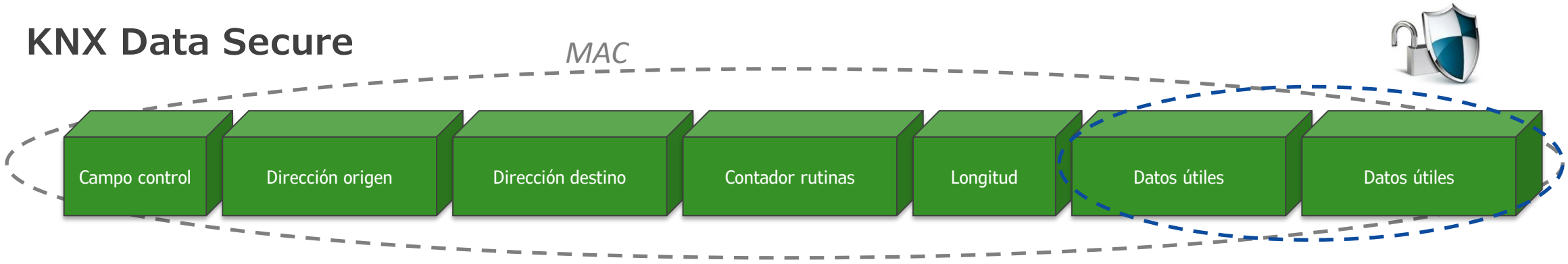
Ejemplo:

Un dispositivo debe enviar un telegrama protegido a otro dispositivo, aunque esté en una línea o incluso área diferente. En este caso, ambos dispositivos deben ser sustituidos por dispositivos con funcionalidad KNX Data Secure.

Dispositivos KNX con y sin funcionalidad KNX Data Secure pueden convivir en una misma instalación.

Medidas de ciberseguridad
KNX Data Secure / KNX IP Secure

KNX Data Secure



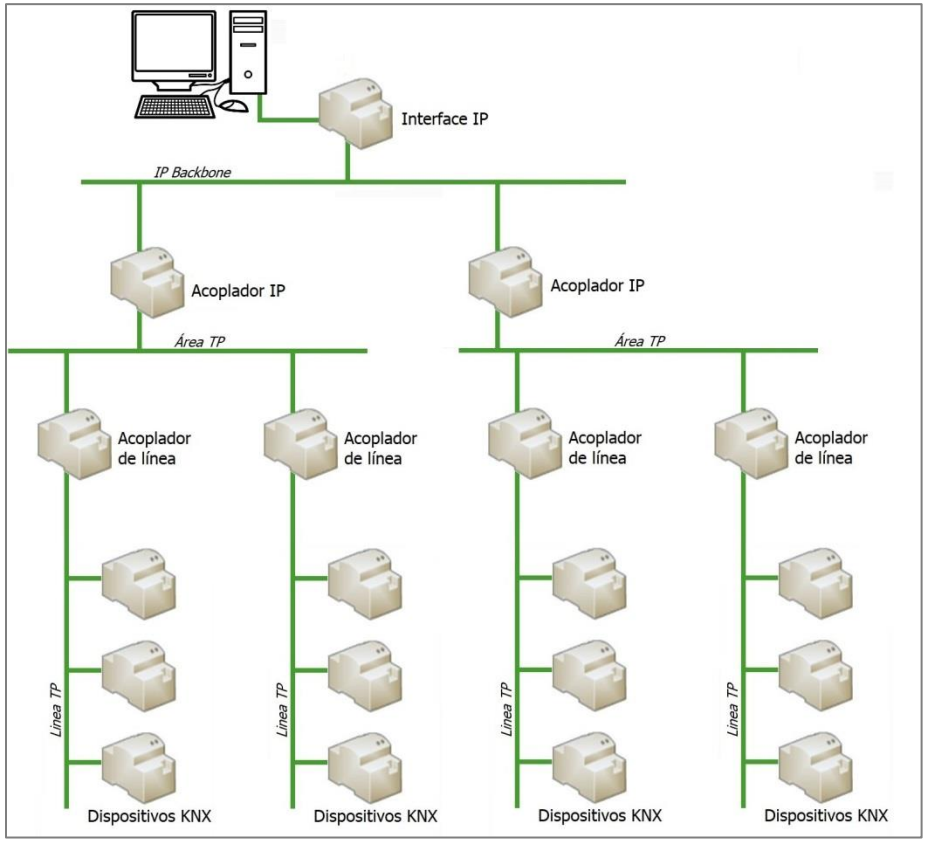
Se encriptan los datos útiles del telegrama KNX (órdenes de actuación, p.ej. encender, apagar, subir, bajar, leer, etc.).

La encriptación es realizada por el dispositivo emisor, y la desencriptación por el dispositivo receptor. Ambos requieren de la funcionalidad KNX Data Secure.

El resto del telegrama no es encriptado, pero asegurado por AES128:
- El telegrama es ampliado por el *Message Authentification Code (MAC)*
- Cualquier manipulación del telegrama provoca una incompatibilidad con el MAC:
  → el telegrama sería inválido

KNX IP Secure

Para la transmisión segura de telegramas vía IP



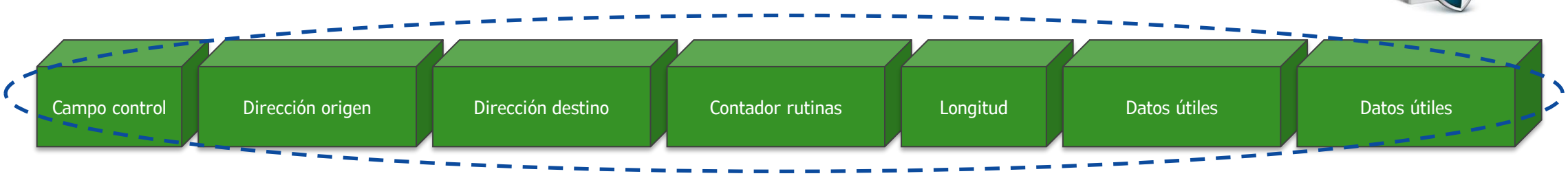
Ejemplo:

Dos instalaciones KNX están conectadas entre sí mediante comunicación IP. Se requiere una transmisión segura de los telegramas.

En este caso, todos los acopladores conectados al IP backbone deben tener la funcionalidad KNX IP Secure.

Medidas de ciberseguridad
KNX Data Secure / KNX IP Secure

KNX IP Secure



Se encripta el telegrama KNX por completo.

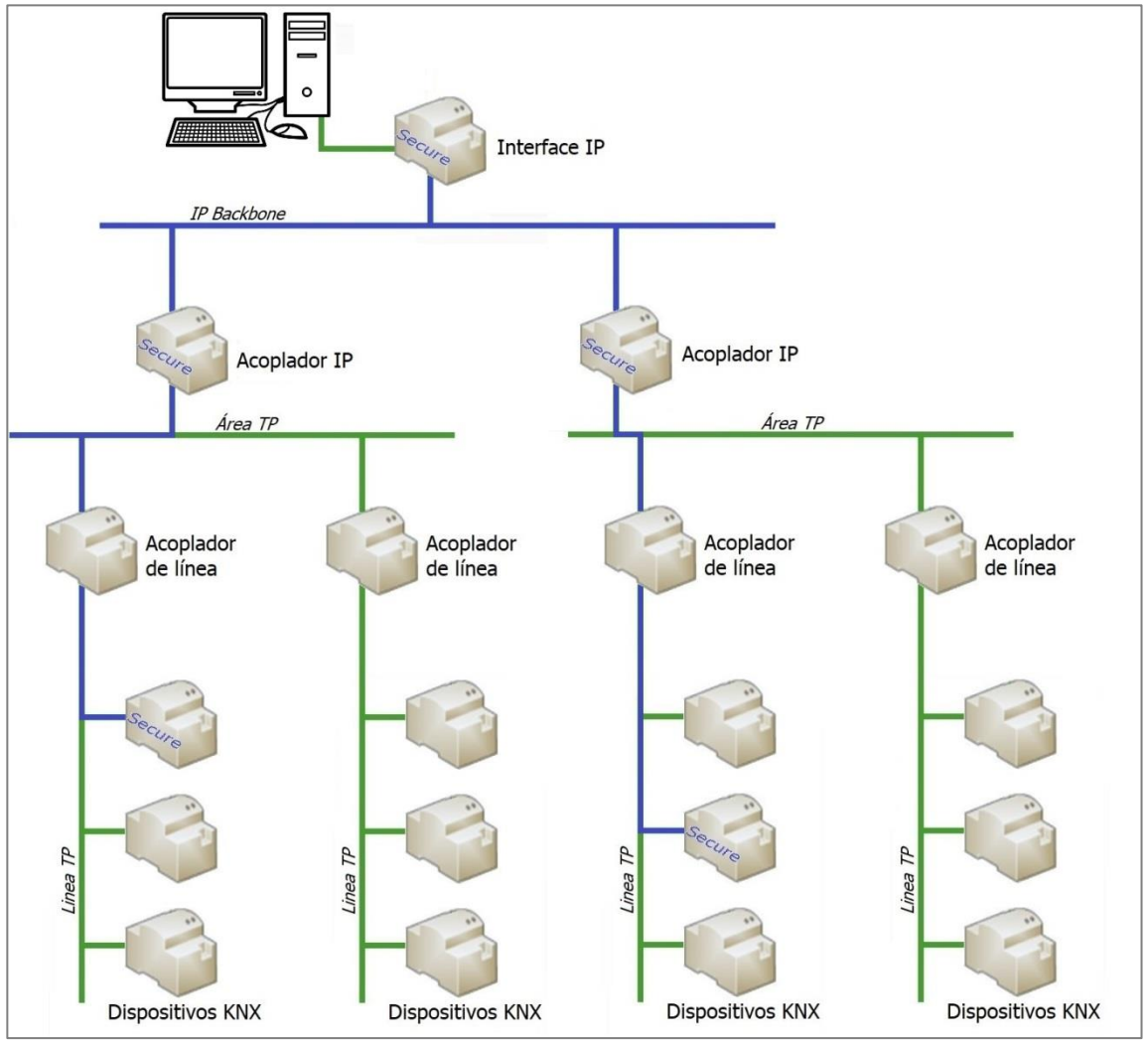
La encriptación es realizada por el enrutador emisor, y la desencriptación por el enrutador receptor. Ambos requieren de la funcionalidad KNX IP Secure.

Ninguna persona no autorizada (es decir, sin la clave AES-128) puede leer la información cuando se transmite p.ej. por internet.

Si una persona no autorizada “inyecta” un telegrama malintencionado no es reconocido por ninguno de los enrutadores.

Medidas de ciberseguridad
KNX Data Secure / KNX IP Secure

KNX Data Secure + KNX IP Secure



KNX Data Secure y KNX IP Secure pueden usarse simultáneamente en una misma instalación KNX.

Resumen

- Cualquier tecnología basada en una comunicación abierta es vulnerable a ser hackeada.

- Existen varios tipos de medidas para proteger una instalación. Hay que analizar proyecto por proyecto qué medidas son las más adecuadas y si son realmente necesarias.

- KNX ofrece varios métodos para aumentar la seguridad de una instalación:
  - Configuración y programación en ETS
  - KNX Data Secure y KNX IP Secure

- Dispositivos con y sin KNX Data Secure pueden convivir en una misma instalación.

- KNX Data Secure y KNX IP Secure pueden convivir en una misma instalación.

- Ambos sistemas aseguran una comunicación segura entre dispositivos KNX, estén en una misma instalación, o a distancia conectados a través de IP:
  - Se impide la infiltración de telegramas manipulados que pretenden obtener el control de la instalación.
  - El método de encriptación AES-128 es uno de los más seguros.

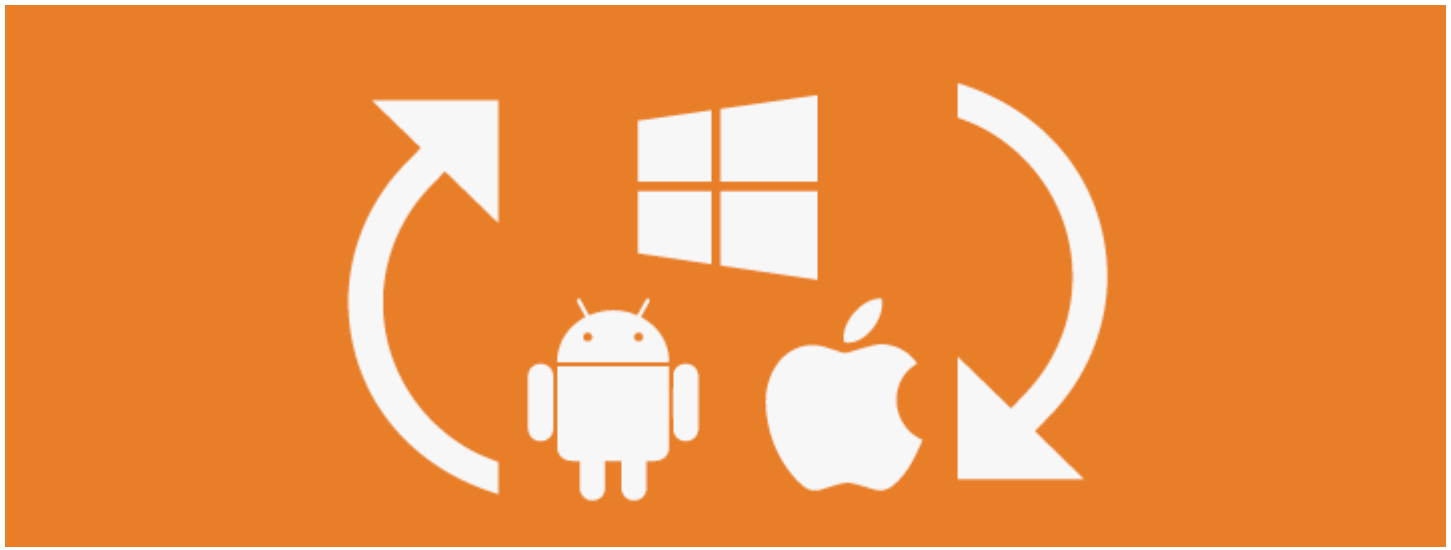
SMART TECHNOLOGY TOPICS

Organizan:

KNX NATIONAL ESPAÑA

SMARTECH CLUSTER

ANTES DE FINALIZAR



- Una de las medidas de seguridad a adoptar por las empresas es la actualización de todos sus equipos y dispositivos. Esto incluye las aplicaciones informáticas y sistemas operativos, el firmware de los equipos electrónicos y los programas antimalware.

- Los parches y actualizaciones son creados por los mismos desarrolladores del software y sirven para mejorar su funcionamiento corrigiendo fallos de seguridad y añadiendo nuevas funciones.

- Las empresas pueden exponerse a importantes riesgos si no realizan actualizaciones en sus aplicaciones y dispositivos. Los ciberdelincuentes pueden usar esa falta de actualización para acceder a los dispositivos e infectarlos, inactivarlos, crear botnets con la finalidad de cometer delitos o robar información confidencial.

¡Muchas gracias por su atención!

SMART TECHNOLOGY TOPICS

Organizan:

KNX NATIONAL ESPAÑA

SMARTECH CLUSTER

Michael Sartor
Asociación KNX España
Secretario Técnico

Mail: info@knx.es
Teléfono: (+34) 934 050 725
Web: www.knx.es

Sergio Hernández
Smartech Cluster
Presidente

Mail:
Teléfono: (+34) 93 182 88 00
Web: www.smartechcluster.org