UNIVERSIDAD DE GRANADA

CIBERSEGURIDAD EN EL INTERNET DE LAS COSAS

Administración de Sistemas y Seguridad

Autor

Pablo Valenzuela Álvarez (pvalenzuela@correo.ugr.es)

ETSIIT
Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

ÍNDICE

1. Introducción

1.1. IoT y su importancia en el mundo actual

El término **Internet de las cosas** (IoT) se refiere a objetos físicos (o un grupo de ellos) que están equipados con sensores, capacidad de procesamiento, software, etc, y que tienen la capacidad de recibir o transferir información a través de redes inalámbricas sin la necesidad de una intervención humana constante, prácticamente mínima.

En el mercado actual, la tecnología IoT se asocia principalmente con productos relacionados con el concepto de "**hogar inteligente**". Este concepto abarca una amplia gama de dispositivos o aparatos, como lámparas u otros dispositivos de iluminación, termostatos, sistemas de seguridad, cámaras de vigilancia y otros electrodomésticos. Todos estos dispositivos pueden ser controlados y monitoreados a través de dispositivos también asociados a ese ecosistema, como por ejemplo un teléfono móvil.

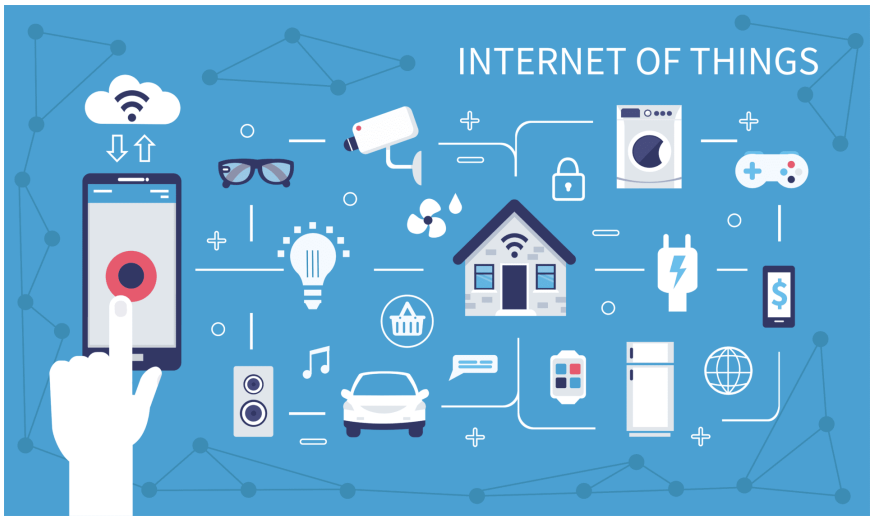

Figura 1: Internet of Things (enlace)

La proliferación de este tipo de productos ha levantado preocupaciones, especialmente en lo que respecta a la **privacidad** y la **seguridad** que estas tecnologías pueden ofrecer. En consecuencia, la industria y los gobiernos han comenzado a tomar medidas para hacer frente a estas preocupaciones, desarrollando normas y marcos regulatorios.

Por ejemplo, en 2018 la Unión Europea aprobó el **GDPR** (reglamento general de protección de datos), en el exige la protección de los datos en cuanto a almacenamiento y administración de personas residentes en la Unión Europea. Aunque esta legislación es local a ciertos países de Europa, tiene un impacto global porque afecta a organizaciones que operan en todo el mundo.

1.2. ¿Por qué es importante la seguridad en IoT?

Como hemos comentado, el IoT abarca un gran conjunto diversificado de elementos. Este grupo genera una ingente cantidad de datos de usuarios, equipos y maquinaria que quedan expuestos y son propensos a ser robados o pirateados por cibercriminales. Si a esto le sumamos el crecimiento exponencial previsto para el futuro como consecuencia de la digitalización de servicios públicos, industria, infraestructuras y ciudades inteligentes, la necesidad de proteger objetos y conexiones resulta vital.

Otro punto a tener en cuenta, es la gran cantidad de información que estos dispositivos son capaces de enviar, a veces sin nuestro consentimiento. Es una característica de estos dispositivos que por el hecho de estar conectados a internet, envían automáticamente información a sus fabricantes.

La ciberseguridad de la información tradicional se centra en el software, pero la seguridad en IoT añade una capa extra de complejidad en la que convergen el mundo cibernético y el mundo físico.

2. Desafíos de seguridad en IoT

Los ataques de ciberseguridad en el entorno IoT pueden amenazar los procesos, la comunicación, el flujo de datos y su almacenamiento. Al estar todo conectado, estos ataques pueden comprometer, por ejemplo, la infraestructura de una pequeña organización, provocando no solo brechas de datos y operaciones no confiables, sino también daños físicos en las instalaciones o a personas dependientes de ellas.

En general, podemos clasificar los ataques en distintas categorías. La primera sería la **suplantación de identidad**, donde se busca hacerse pasar por otra persona, normalmente el autor del programa, para así modificar las funciones y operaciones del dispositivo. La segunda categoría es la **revelación de información**, en la que un atacante busca obtener información para la que no tiene autorización y enviar datos falsos. Otras categorías incluyen la provocación de **alteraciones**, ya sea en un dispositivo físico o en el software que ejecuta, la **denegación de servicio** mediante ataques que imposibilitan la conexión de equipos o sistemas a la red, y la **elevación de privilegios** en un dispositivo, forzandolo a hacer otra función diferente de la que estaba programado originalmente.

2.1. Principales amenazas y riesgos de seguridad en IoT

El IoT presenta riesgos inherentes a su propia naturaleza, como son la **conectividad**, la **recolección de datos**, las **vulnerabilidades técnicas** en los mecanismos de autenticación y limitaciones de cálculo. Otro factor importante de estos dispositivos es que su ciclo de vida suele ser muy corto por lo que quedan obsoletos y sin soporte poco tiempo después de que se haya completado su despliegue.

Considerando estas características, podemos hacer una lista de las amenazas de seguridad más habituales en IoT, clasificándolas entre las que afectan a dispositivos, conectividad y datos, aunque siempre suelen estar relacionadas.

2.1.1. Vulnerabilidad en el software

Una de las principales vulnerabilidades encontradas en el software de los dispositivos IoT tiene que ver con las **credenciales** de administración. En algunos dispositivos, no es posible modificar las credenciales que vienen dados por defecto, lo que supone un grave riesgo ya que generalmente estas son de dominio público y cualquier ciberdelincuente las puede obtener directamente de la documentación del fabricante.

Las credenciales de acceso embebidas o la existencia de cuentas con privilegios utilizadas por el fabricante y no documentadas suponen el mismo riesgo.

Además, los dispositivos IoT no están exentos de sufrir otro tipo de vulnerabilidades como el desbordamiento de buffer, condiciones de carrera (cuando un dispositivo intenta realizar dos o más operaciones al mismo tiempo), denegaciones de servicio, etc.

2.1.2. Ataque sobre contraseñas y credenciales

Como hemos comentado en el punto anterior, muchos dispositivos IoT vienen configurados con contraseñas por defecto muy inseguras y, aunque el dispositivo permite cambiarla, muchos usuarios no lo saben. Este tipo de contraseñas exponen al dispositivo a los ataques por **fuerza bruta**, es decir, los intentos de descifrar la clave probando todas las combinaciones posibles hasta encontrar la correcta. En este tipo de ataques se suelen usar diccionarios o las llamadas **tablas arcoiris**.

2.1.3. Acceso físico al dispositivo

Los sistemas que se encuentran en exteriores, como cámaras de vigilancia y sensores IoT instalados en contadores o farolas y otros casos, pueden sufrir ataques. Los dispositivos situados en interiores, ya sea de una oficina, una nave industrial o viviendas también son susceptibles a recibir accesos físicos aunque este riesgo sea menor.

Figura 2. El acceso físico a un dispositivo IoT es una amenaza a tener en cuenta (enlace)

2.1.4. Conexión a internet

Muchos dispositivos IoT están conectados a internet y este es uno de los principales puntos débiles que poseen. Existen buscadores como **Shodan** [4], cuyo objetivo es encontrar dispositivos y servicios accesibles desde internet. Mediante el uso de estos buscadores, podemos encontrar “cosas” como cámaras IP, contadores inteligentes, etc, conectados a internet y averiguar detalles sobre su configuración.

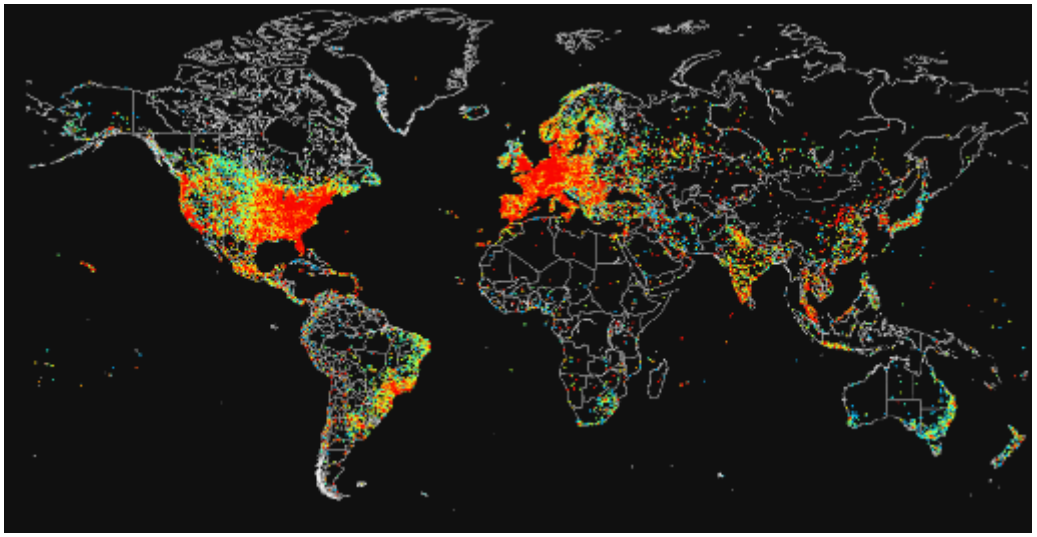

Figura 3. Mapa de dispositivos IoT (enlace)

Cuando un ciberdelincuente consigue acceder a múltiples dispositivos, esta red se denomina botnet, y cada dispositivo en ella es un bot o zombi. Con este tipo de redes se pueden efectuar acciones maliciosas como robar información, difundir spam, malware o realizar ataques DDoS.

2.1.5. Ataques DDoS

Los ataques de denegación de servicio distribuido (**DDoS**) pueden realizarse por dispositivos IoT infectados.

Estas “cosas” secuestradas se utilizan como base de ataque para infectar más “cosas” o esconder una actividad maliciosa. Estos ciberataques consisten en saturar un servicio enviando peticiones masivas de conexión al mismo tiempo. Denegar un servicio supone también dejar a un aparato inoperativo y en muchos casos no se soluciona el problema reiniciando o restaurando el software.

Aunque este tipo de amenaza suele dirigirse hacia las organizaciones, también pueden afectar a hogares inteligentes.

2.1.6. Malware y ransomware

Los ataques de **malware** (ataques que realizan acciones dañinas sobre un software o usuarios) y **ransomware** o secuestro de datos (ataques que restringen el acceso a determinados sistemas y que piden un "rescate" a cambio de quitar esa restricción) se han incrementado bastante debido al aumento de dispositivos IoT conectados en los últimos años. Entre las variantes más comunes se encuentra el malware botnet de IoT.

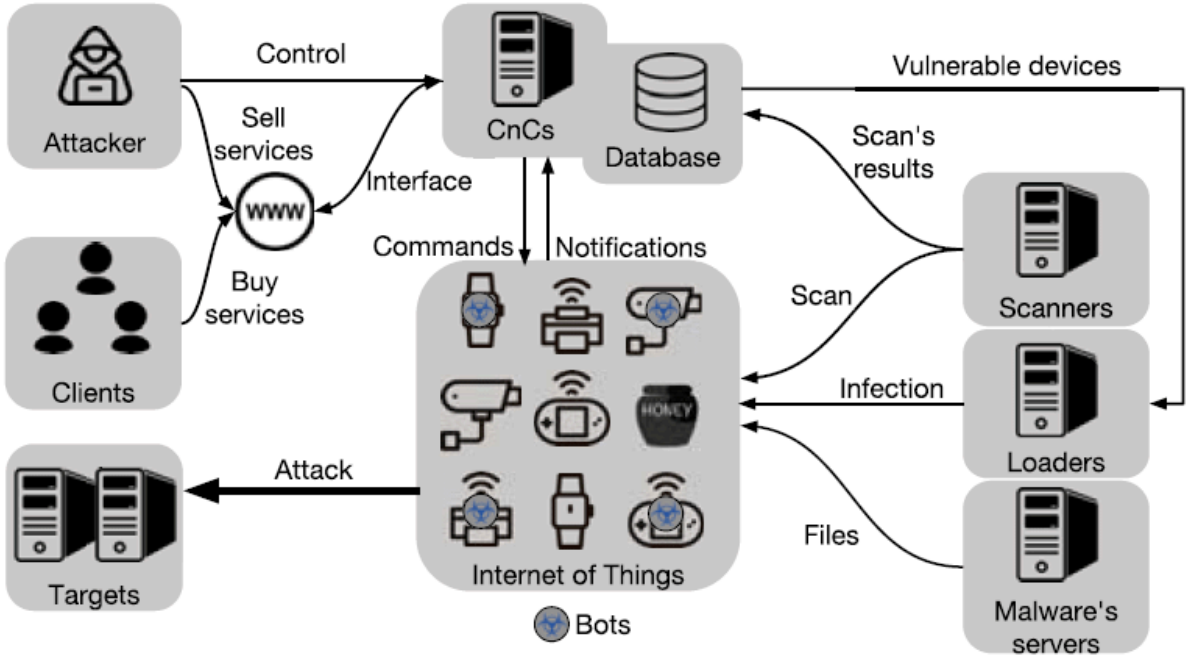

Figura 4. Procedimiento de ataque botnet IoT (enlace)

2.1.7. Interceptación de datos de tránsito

La transmisión de datos es algo fundamental en los dispositivos IoT. Están diseñados para interactuar con el mundo físico, siendo el envío o recepción de datos su razón de funcionamiento.

Si un ciberdelincuente consigue acceso a la red local o LAN donde se encuentra el dispositivo o el receptor de información, podría acceder a esta o modificarla. A este tipo de ciberataques se les conoce como Hombre en el medio (man in the middle) o **MitM** por sus siglas en inglés.

Hay dos tipos de variantes cuando un atacante realiza un MitM:

- **MitM pasivo**: Se intercepta el tráfico y se envían los datos sin alterar, de esta manera se pueden obtener datos sensibles e información confidencial de la empresa.

- **MitM activo**: Se intercepta y se modifica el tráfico antes de enviarlo nuevamente, es decir, altera la información recibida por el usuario.

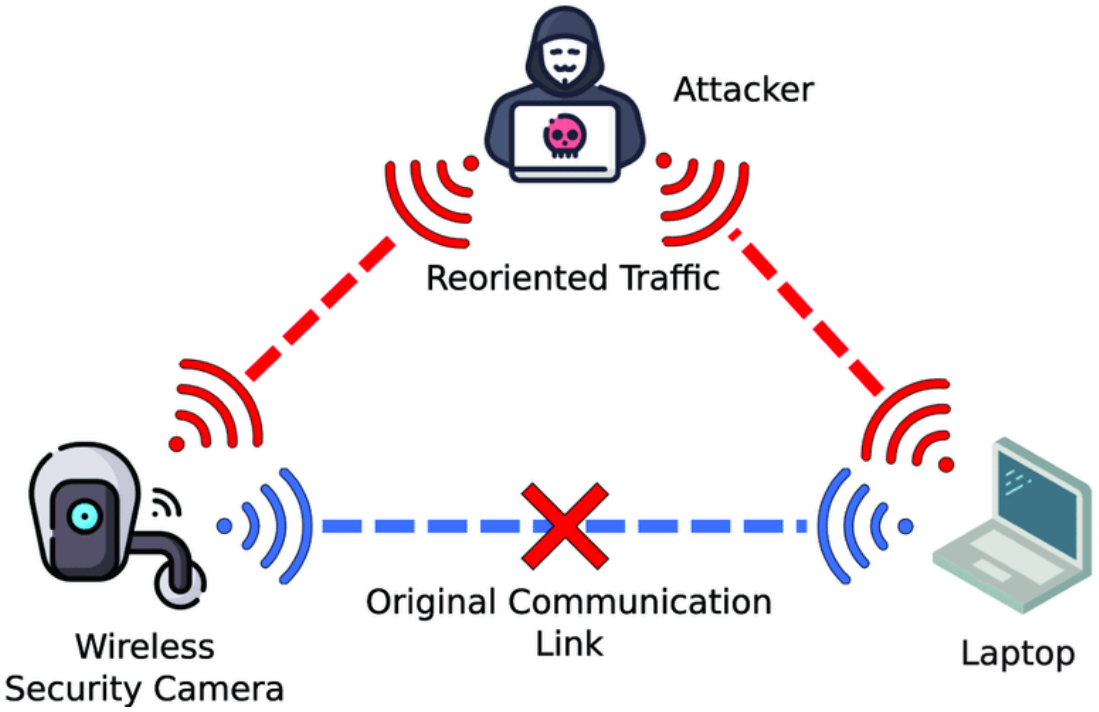

Figura 5. Ejemplo de MitM en una cámara de seguridad (enlace)

2.1.8. Ataques basados en hardware

Si no se ha tenido en cuenta la seguridad en el diseño de un objeto que se conectará a la red, se corre el riesgo de que el objeto sea blanco de ataques durante su funcionamiento.

Muchos dispositivos IoT no aplican los principios de **mínimo privilegio**. Si estos principios se aplicaran de fábrica, el dispositivo proporcionaría una funcionalidad básica para su administración y operación, haciendo que cualquier uso inseguro sea una decisión consciente del usuario. Sin embargo, al incorporar este tipo de seguridad por defecto, no se debe descuidar la experiencia de usuario. Si los mecanismos de seguridad dificultan el uso normal, el usuario encontrará maneras de evitarlos.

Algunos fabricantes pueden dejar habilitados servicios o herramientas que el aparato o el usuario no necesite para un uso normal. Cuantos más servicios estén instalados y habilitados, mayor será la probabilidad de que alguno de ellos tenga una vulnerabilidad que pueda ser explotada por los ciberdelincuentes.

2.1.9. Acceso a la plataforma de administración

Muchos dispositivos IoT, debido a su tamaño, no cuentan con elementos que permitan interactuar directamente con ellos, como pantallas o teclados. En su lugar, suelen utilizar **interfaces web** o **aplicaciones móviles** para su administración. Si una de estas opciones cuenta con alguna vulnerabilidad o carece de las medidas de seguridad necesarias para evitar accesos no autorizados, los ciberdelincuentes podrían acceder a ella y controlar el dispositivo.

2.1.10. Ataques sobre la privacidad de los datos

La información que manejan los dispositivos IoT es de suma importancia. La obtención de datos personales, historial médico, claves de cerraduras y cuentas bancarias, etc, puede ser utilizada por ciberdelincuentes para su propio beneficio o para venderla, comprometiendo así la privacidad y seguridad de los afectados.

3. Ejemplos de problemas de seguridad de IoT en empresas

En esta sección, mostraremos algunos de los casos más relevantes en los que dispositivos o componentes IoT han sido atacados por cibercriminales, ocasionando grandes problemas a empresas u organizaciones. Estos incidentes subrayan las vulnerabilidades inherentes a la IoT y la urgencia de implementar medidas de seguridad efectivas.

3.1. Stuxnet (2010)

Stuxnet fue considerado el primer gusano en atacar sistemas de control industrial. Su objetivo era el de sabotear los procesos de enriquecimiento de uranio del programa nuclear iraní. Se estima que destruyó hasta mil máquinas centrifugadoras de la planta antes de ser descubierto.

3.2. Ataque a la Oficina Federal de Seguridad de Información en Alemania [5] (2010)

La Oficina Federal de Seguridad de Información de Alemania emitió un informe en el que confirmaba que un grupo de hackers había accedido sin autorización y había impedido el apagado de uno de los hornos en una empresa de acero, lo cual provocó un daño masivo a la instalación.

3.3 Robo de información en la empresa Calpine [6] (2013)

En 2013 se confirmó que grupos supuestamente vinculados con la inteligencia iraní, robaron información de la empresa Calpine. Los datos incluían planos detallados de la red y de 71 estaciones eléctricas, la ubicación precisa de dispositivos, diagramas de red y contraseñas de dispositivos. Este robo de información permitió ataques posteriores como la infiltración en el sistema de una presa a través de un módem.

3.4. Botnet Mirai [7,8] (2016)

En septiembre de 2016, la botnet Mirai lanzó un ataque DDoS contra el sitio web de un conocido experto en seguridad. Una semana más tarde, se publicó su código fuente, lo que permitió a otros ciberdelincuentes replicarlo. Se cree que las interrupciones de funcionamiento en servicios como Twitter, Airbnb, Reddit, Amazon, Spotify, Netflix, etc, en octubre de 2016 fueron debido al uso de esta botnet.

Mirai funcionaba escaneando Internet en busca de dispositivos IoT que se ejecutan con el procesador ARC (versión reducida de Linux), y aprovechando la configuración por defecto que permitirá acceso al dispositivo e infectarlo.

Aunque se detuvo a los autores originales, su código fuente sigue vivo y generando múltiples variantes como IoTrooper y Reaper.

3.5. Botnet Persirai [9] (2017)

En 2017, surgió la botnet denominada Persirai, que dirigía sus ataques hacia más de mil modelos de cámaras IP de distintos fabricantes. Se descubrió que había infectado a aproximadamente 120000 dispositivos a través de Shodan.

Las cámaras IP suelen usar protocolos Universal Plug & Play (UPnP), que son protocolos de red que permiten abrir un puerto en el router y actuar como un servidor, lo que los hace objetivos visibles para el malware. Los usuarios deben deshabilitar estos protocolos para evitar que los dispositivos abran puertos a internet sin ninguna advertencia. Aunque esta responsabilidad también recae sobre los fabricantes, que deberían garantizar que sus productos son seguros y siempre están actualizados.

3.6. Malware VPNFilter [10] (2018)

Se estima que el malware VPNFilter infectó a más de medio millón de enrutadores en más de cincuenta países. Dicho programa puede instalar malware en los dispositivos conectados a un enrutador y recopilar la información que pasa, bloquear el tráfico de red y robar contraseñas.

Los principales objetivos de este malware son ASUS, D-Link, Huawei, Ubiquiti, UPVEL y ZTE, así como los nuevos modelos de Linksys, MicroTik, Netgear y TP-Link.

3.7. Pirateo del Tesla Model X [11] (2020)

Un experto en ciberseguridad aprovechó una vulnerabilidad del Bluetooth para clonar la llave que se usa en el modelo Tesla Model X en apenas 90 segundos. Utilizando los últimos cinco dígitos del bastidor, que están visibles en el parabrisas del vehículo, el experto fué capaz de clonar la llave electrónica y obtener acceso al coche. Este incidente destacó la importancia de reforzar la seguridad de los sistemas de acceso sin llave para evitar tales vulnerabilidades.

3.8. Pirateo de las cámaras de Verkada [12] (2021)

En 2021, la empresa de cámaras de seguridad Verkada sufrió un ataque por parte de hackers suizos, exponiendo alrededor de 150,000 transmisiones en directo de sus cámaras. Entre los afectados se encontraban servicios públicos como escuelas, hospitales y prisiones, así como empresas privadas como Tesla y Cloudflare. Además del metraje en la cámara, el grupo de hackers afirma que consiguió también acceder a la lista completa de clientes de la empresa Verkada y su información financiera.

4. Conclusión

En el mundo de la Internet de las Cosas (IoT), la seguridad emerge como una preocupación ineludible. A medida que la interconexión de dispositivos y la recopilación de datos se vuelven ubicuos, el riesgo de vulnerabilidades y ataques cibernéticos se incrementa exponencialmente. Sin embargo, tras analizar detenidamente las mejores prácticas y consejos proporcionados por diversas fuentes, queda claro que la seguridad en IoT no es una meta inalcanzable, sino más bien un proceso continuo que requiere atención constante.

Uno de los pilares fundamentales para salvaguardar la seguridad en entornos IoT es mantener actualizados tanto los dispositivos como el software que los respalda. Este simple pero vital paso asegura que las últimas correcciones de seguridad se implementen de manera oportuna, mitigando así posibles vulnerabilidades explotadas por cibercriminales.

Además, la concienciación del usuario emerge como una herramienta poderosa en la lucha contra los ciberataques. Educar a empleados y usuarios sobre buenas prácticas de ciberseguridad, desde el uso de contraseñas robustas hasta la identificación de correos electrónicos sospechosos, fortalece la primera línea de defensa contra amenazas digitales.

La segmentación de redes y el uso de VPNs (Redes Privadas Virtuales) añaden capas adicionales de protección, limitando el acceso no autorizado a dispositivos IoT y protegiendo las comunicaciones sensibles. Asimismo, la configuración adecuada de cortafuegos y la vigilancia constante de la red son imprescindibles para mantener la integridad de los sistemas conectados.

En última instancia, la seguridad en IoT no es un desafío que pueda abordarse de manera aislada, sino más bien como un esfuerzo conjunto que involucra a fabricantes, proveedores, usuarios y organismos reguladores. Solo adoptando un enfoque integral y proactivo hacia la seguridad, podemos mitigar los riesgos asociados con la creciente proliferación de dispositivos IoT y garantizar un futuro digital más seguro y confiable.

5. Referencias

[1]. “Internet de las cosas.” *Wikipedia*, https://es.wikipedia.org/wiki/Internet_de_las_cosas.

[2]. “¿Qué es IoT y cómo está transformando nuestras vidas?” *Linkedin*, https://www.linkedin.com/pulse/qu%C3%A9-es-iot-y-c%C3%B3mo-est%C3%A1-transformando-nuestras-vidas-telefonica/.

[3]. “Seguridad en IoT, riesgos y desafíos de la Internet de las Cosas.” *Redes & Telecom*, https://www.redestelecom.es/especiales/seguridad-en-iot-riesgos-y-desafios-de-la-internet-de-las-cosas/.

[4]. “Search Engine for the Internet of Everything.” *Shodan Search Engine*, https://www.shodan.io/.

[5]. “Ciberataque a metalúrgica en Alemania y la seguridad física en empresas.” *Seguridad digital*, https://www.welivesecurity.com/la-es/2014/12/23/ciberataque-metalurgica-alemania-seguridad-fisica-en-empresas/.

[6]. “Iranian hackers infiltrated U.S. power grid, dam computers.” *CBC*, https://www.cbc.ca/news/science/hackers-infrastructure-1.3376342.

[7]. “¿Qué es la botnet Mirai?” *Cloudflare*, https://www.cloudflare.com/es-es/learning/ddos/glossary/mirai-botnet/.

[8]. “Botnet Mirai: ¿nuestros electrodomésticos pueden atacarnos?” *WeLiveSecurity*, https://www.welivesecurity.com/es/seguridad-iot/botnet-mirai-electrodomesticos-pueden-atacarnos/.

[9]. “Persirai: nueva red botnet de IoT que infecta las cámaras IP | Redes&Telecom.” *Redes & Telecom*, https://www.redestelecom.es/seguridad/persirai-nueva-red-botnet-de-iot-que-infecta-las-camaras-ip/.

[10]. “200.000 routers más podrían estár infectados por VPNFilter.” *RedesTelecom*, https://www.redestelecom.es/seguridad/200-000-routers-mas-podrian-estar-infectados-por-vpnfilter/.

[11]. “Tesla Model X Has Flaw Allowing It to Be Hacked and Stolen.” *Car and Driver*, https://www.caranddriver.com/news/a34762383/tesla-model-x-hack-steal/.

[12]. “Security startup Verkada hack exposes 150000 security cameras in Tesla factories, jails, and more.” *The Verge*, https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals.