
Desliza
IOT
INTERNET
OF THINGS
Ingrid Mora
Consultora

El Internet de las Cosas

IOT

Desliza →

WAFRA

Ingrid Mora
Consultora

Qué es?

1

(IoT, por sus siglas en inglés) se refiere a una red de objetos físicos ("cosas") equipados con sensores, software y otras tecnologías que se conectan e intercambian datos con otros dispositivos y sistemas a través de Internet, permitiendo la automatización, monitoreo y control remoto de dispositivos cotidianos e industriales.

Ingrid Mora Consultora

Cómo funciona?

2

Los dispositivos IoT recopilan datos del entorno (temperatura, movimiento, humedad y otros) mediante sensores y los transmiten a la nube o a otros sistemas para su análisis y acción.

Ejemplos:

Electrodomésticos inteligentes, relojes inteligentes, wearables de salud y asistentes de voz, maquinaria industrial.

Aplicaciones industriales (IoT):

Mantenimiento predictivo, agricultura de precisión, gestión de inventarios, ciudades inteligentes y automatización de procesos.

Ingrid Mora
Consultora

Datos Reales

3

1.5

Billones de intentos de ataques anuales IoT

A nivel global, los ataques a dispositivos IoT (como controladores de generadores y sistemas de monitoreo de AC) superan ya los 1.5 billones de intentos anuales.

Ingrid Mora Consultora

Casos Reales

El Casino y la Pecera

4

Este es el caso más famoso de cómo un dispositivo insignificante puede quebrar una corporación.

El ataque: Un casino de lujo tenía una pecera inteligente en su lobby que permitía controlar la temperatura y el alimento vía Wi-Fi.

La brecha: Los atacantes entraron a través del sensor de la pecera porque no tenía seguridad robusta. El termómetro estaba conectado a la red principal del casino para que el personal pudiera monitorearlo. No había segmentación de red.

El resultado: Una vez dentro de la pecera, saltaron a la red principal del casino y exfiltraron 10 GB de datos de su base de datos de "jugadores de alto nivel" (High Rollers) hacia la nube.

Lección: La red no estaba segmentada. La pecera "veía" directamente los servidores financieros.

Ingrid Mora
Consultora

Casos Reales

El caso "TLStorm"

5

En 2022, la firma de seguridad Armis descubrió tres vulnerabilidades críticas que afectaban a millones de unidades Smart-UPS de la marca APC (una de las más usadas en Costa Rica).

El ataque: Los atacantes podían tomar el control total del dispositivo a través de internet sin necesidad de contraseñas.

El impacto: Podían apagar de golpe centros de datos completos, pero lo más grave es que podían quemar físicamente la UPS. Al manipular el voltaje y los ciclos de carga, podían causar que las baterías se incendiaran o explotaran.

Evidencia: Schneider Electric (dueña de APC) tuvo que emitir parches de emergencia globales porque el riesgo de daño físico a infraestructuras críticas era inminente.

Casos Reales

El ataque a Target

6

Este es el caso más famoso de la historia sobre cómo un sistema de HVAC (Aire Acondicionado) destruyó a un gigante del retail.

El ataque: Los hackers no atacaron a Target directamente. Atacaron a Fazio Mechanical Services, una empresa pequeña que brindaba mantenimiento al aire acondicionado de las tiendas.

La brecha: Robaron las credenciales que los técnicos usaban para monitorear remotamente la temperatura de las tiendas. Como el sistema de refrigeración estaba conectado a la red principal de la empresa, los hackers saltaron desde el termostato hasta los puntos de venta (POS).

El resultado: Robaron los datos de 40 millones de tarjetas de crédito y débito. Target tuvo que pagar más de **18.5 millones de dólares en multas y acuerdos legales.**

Ingrid Mora
Consultora

En Resumen

Target aprendió la lección por las malas.

Vos podés aprenderla por estrategia. Si no sabés exactamente qué dispositivos están "hablando" en tu red ahora mismo, el próximo podría ser tu empresa.

La auditoría no es una opción, es tu única defensa.

WAFRA

Contáctame
imora@wafratransformation.com