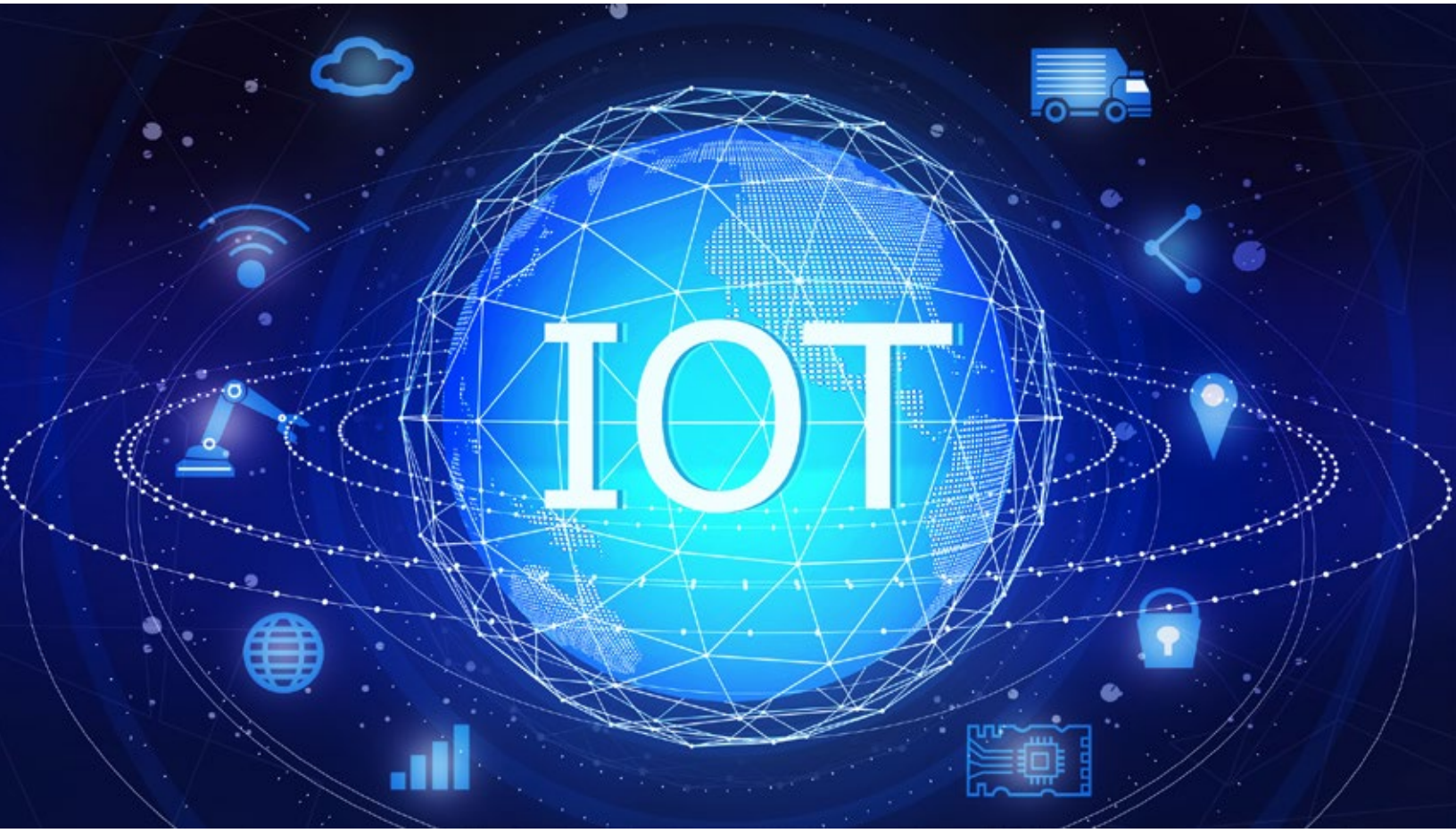
CENTRO
DE COMPETENCIAS
TECMILENIO

Las brechas de datos

Las brechas de datos



Los sistemas de Internet de las cosas IoT, están revolucionando la forma en la que interactuamos con el mundo y la manera en que las empresas manejan sus operaciones. Sin embargo, estos sistemas también presentan una serie de desafíos y riesgos relacionados con la privacidad y seguridad de los datos manejados en estos sistemas.

Esto se debe a que actores malintencionados vulneran estos sistemas por una gran cantidad de motivos, estos usualmente agrupados por el perfil del atacante, los cuales pueden ser categorizados en cuatro grupos: entidades patrocinadas por naciones, individuos con conocimiento del funcionamiento de estos sistemas, individuos o grupos con intenciones de lucrar y otros dispositivos infectados con algún virus que se propaga automáticamente.

Los más prominentes en el espacio del IoT suelen ser los grupos patrocinados por naciones extranjeras, Rusia, China y Corea, pues estos vulneran sistemas IoT con la finalidad de atacar a la infraestructura de los países atacados y en el proceso roban información confidencial para pasarla a las autoridades correspondientes de dichos países o en su defecto la venden en mercados del bajo mundo a cambio de grandes sumas de criptomonedas, de acuerdo con Ribeiro (2023).

Los ataques realizados por insiders o individuos con conocimiento de una solución de IoT también son otro perfil de atacante bastante importante, pues al tener información confidencial del funcionamiento de estos dispositivos pueden orquestar operaciones indetectables por otros expertos, aunque lo más común

es que sean contratados por naciones externas, o individuos afiliados a grupos de cibercrimen con la finalidad de extraer información confidencial, según Haji (2019).

Los individuos o grupos de hackers son otro de los perfiles de atacantes más comunes y en concreto se relaciona con el cuarto, es decir, virus auto propagables a dispositivos IoT, esto se debe a que estos virus suelen ser programados por los individuos o grupos sin un trasfondo en concreto pero con el interés de lucrar tanto de la información obtenida de los sistemas como de comprometer los sistemas IoT para controlarlos, según Tobok (2019).

Una de las principales preocupaciones en cuanto a la privacidad de los datos se refiere son las brechas de datos. Las brechas de datos son la exposición no autorizada de información confidencial, lo que puede ser utilizado por terceros para causar daño, lucrar con esta información, o desprestigiar a una empresa. En el contexto de IoT, las brechas de datos pueden ocurrir debido a varias razones, incluyendo el robo de dispositivos, la explotación de vulnerabilidades en los sistemas de seguridad y la falta de encriptación de los datos transmitidos.

Dependiendo del sector afectado las brechas pueden variar de exponer información como correos, teléfonos, contraseñas de personas, a exponer información de operaciones internas de gobiernos.

Un caso de una brecha donde se expuso información confidencial, más no existieron daños graves, fue la filtración de octubre de 2012 de pagos de streamers de Twitch donde un individuo o grupo no identificado accedió a servidores mal configurados y extrajo esta información, sin embargo los detalles de inicio de sesión como contraseñas, correos o incluso detalles de facturación o de residencia no fueron vulnerados.

Este no es un ataque a sistemas IoT en sí, sin embargo, remarca el tipo de información que es resguardado en sistemas computacionales, según Micheli y Tsiaoussidis (2022).

Otro caso de brecha de información que involucraba a dispositivos IoT ocurrió en mayo de 2019, cuando Vince Steckler, en ese entonces jefe ejecutivo de Avast (una marca de software de antivirus), reportó que existían ciertas vulnerabilidades en dispositivos IoT presentes en una gran variedad de dispositivos domésticos como lo eran cafeteras, focos y televisiones. En concreto estos dispositivos IoT requieren de una aplicación o medio de control instalado en un dispositivo móvil para funcionar, o en el caso de una televisión únicamente que fuera inteligente. Pero tras infectar los dispositivos IoT, los atacantes mandaban virus a los dispositivos móviles por medio de la app de control, lo cual les daba acceso a toda la información de los dispositivos móviles vulnerando la privacidad de los usuarios, según Parker (2019).

Un caso de brecha de seguridad gubernamental ocurrido en México en 2022 fue cuando se revelaron datos del estado de salud del presidente Andrés Lopez Obrador, el cual se encontraba grave y había acudido al hospital en un traslado de emergencia, sin embargo, también se filtraron documentos que se remontaban hasta el año 2016. Esta filtración fue realizada por un grupo hacktivista, es decir, sin afiliación política o búsqueda de fines de lucro llamado guacamaya, el cual se dedicaba a exponer gobiernos de América hispanoparlante. Este tipo de perfiles de atacantes no es tan común en la actualidad, sin embargo, el ejemplo más importante de este perfil fue el del grupo hacktivista anonymous, aunque en realidad este era una bandera bajo la que cualquier individuo se podía escudar para cometer ciberdelitos con intenciones humanas y teóricamente de buena fe, según Infobae (2022).

Estos son tan solo algunos casos que han ocurrido los cuales demuestran la importancia de buenas medidas de prevención y mitigación de ciberataques. Además se demuestra la importancia de añadir diversas capas de seguridad para proteger la información que los sistemas computacionales maneja, sobre todo los sistemas IoT pues estos se encuentra en cada sector de la industria moderna y nos dejan en claro que incluso aparatos como tostadoras, cafeteras o microondas pueden recopilar una gran cantidad de información la cual en manos equivocadas puede causar mucho daño.

Referencias bibliográficas

- Ribeiro, A. (2023). *ODNI report assesses potential cyber threats from China, Russia, Iran, North Korea that challenge US defenses. Industrial Cyber*. Recuperado de https://industrialcyber.co/reports/odni-report-assesses-potential-cyber-threats-from-china-russia-iran-north-korea-that-challenge-us-defenses/
- Haji, S. (2019). *How IoT Opens the Door for Insider Attacks Against Industrial Infrastructure.* Recuperado de https://www.securityweek.com/how-iot-opens-door-insider-attacks-against-industrial-infrastructure/
- Tobok, D. (2019). *EVERYTHING YOU NEED TO KNOW ABOUT BOTNETS. cypfer*. Recuperado de https://cypfer.com/everything-you-need-to-know-about-botnets/
- Micheli, M., y Tsiaoussidis, A. (2022). *Full list of all Twitch payouts (Twitch leaks). Dot Sports*. Recuperado de https://dotesports.com/streaming/news/full-list-of-all-twitch-payouts-twitch-leaks
- Parker, C. (2019). *CYBER SNAG Hackers can steal your ID and bank details from Whatsapp, smart TVs and even COFFEE MACHINES, security expert warns. The Sun*. Recuperado de https://www.thesun.co.uk/news/9106976/hackers-steal-bank-details-whatsapp-smart-tvs-coffee-machines-expert/
- infobae. (2022). *Sedena sufrió hackeo: se filtraron miles de documentos confidenciales del gobierno de AMLO. infobae*. Recuperado de https://www.infobae.com/america/mexico/2022/09/30/sedena-sufrio-hackeo-se-filtraron-miles-de-documentos-confidenciales-del-gobierno-de-amlo/