Riesgos del IoT

Como he mencionado en mis entradas previas, el IoT ofrece un gran número de ventajas y comodidades tanto a los individuos como a las empresas. Pero al igual que con la gran mayoría de tecnologías, también hay que tener en cuenta los riesgos que conlleva utilizar dispositivos IoT o cualquier otra tecnología en general. Hay que tener en cuenta, que la mayoría de estos riesgos estarán relacionado con la seguridad.

El primer riesgo del que voy a hablar se encuentra en los fabricantes de dispositivos IoT. Al igual que todas las compañías, las empresas que diseñan dispositivos IoT están orientadas a los beneficios y al tiempo de comercialización. Esto hace que al diseñar un dispositivo pasen por alto algunas consideraciones de seguridad necesarias para el mismo. Esto permite a un atacante acceder a la información del dispositivo con un mínimo esfuerzo. Cabe destacar que esta información puede ser desde transmisiones de video y audio, hasta correos electrónicos y contraseñas. También, estos dispositivos mal diseñados permiten la ejecución de comandos remotos que pueden reprogramar el firmware del dispositivo [1].

El segundo riesgo que lastra el IoT son las *botnets*. Si los dispositivos IoT no tienen las medidas de seguridad apropiadas pueden ser infectadas por distintos tipos de malware. Si bien es cierto que un dispositivo infectado no significa un riesgo, el gran número de dispositivos conectados a internet sin seguridad si lo es. Es importante destacar que los dispositivos IoT son más vulnerables a ser infectados por un fragmento de software malicioso debido a que no reciben actualizaciones de seguridad regularmente [2]. Un gran número de dispositivos IoT es capaz de poner en peligro instalaciones críticas de nuestro día a día, o que suceda algo similar a la botnet DDoS Mirai de 2016 [3]. Finalmente es necesario destacar que los dispositivos IoT han tenido el segundo porcentaje de infección más alto entre todas las plataformas,

siendo de un 32.72% [4].

Otro riesgo que pueden generar los dispositivos conectados a la red es la perdida de privacidad y confidencialidad. Un gran número de terceros pueden utilizar este tipo de dispositivos para invadir la privacidad tanto de individuos como de organizaciones. Es necesario destacar que este grupo de terceros pueden ser los crackers (termino negativo del hacker), los gobiernos o los competidores empresariales. Si consiguen acceder a la información, ya sea de carácter confidencial o general, lo más probable es que esta información se utilice sin el permiso ni el consentimiento del propietario. Un par de ejemplos de esta pérdida de privacidad y confidencialidad serían los siguientes [2]:

- Obtener el control de una cámara de seguridad para conocer los hábitos del objetivo.
- Empezar a obtener datos de varios dispositivos IoT y utilizar los datos recogidos para extorsionar a la compañía o para vendérselos a compañías competidoras en el mercado negro.

El siguiente riesgo que voy a mencionar sobre el IoT es la visibilidad de los dispositivos en internet. El éxito de un ataque a dispositivos IoT está muy relacionado a la visibilidad que el dispositivo tiene en internet. Como he mencionado anteriormente en este artículo, los dispositivos IoT son propensos a estar infectados y empiezan a formar parte de una botnet. Esto es debido a que muchos dispositivos están conectados con direcciones IP públicas, haciendo a dichos dispositivos vulnerables ante prácticamente cualquier ataque. Para reducir la infección, entre otras técnicas se encuentra contar con un traductor de redes (NAT). Emplear esta técnica reduce el número de dispositivos visibles al escanear una red.

Para finalizar este post, me gustaría concluir y resumir un poco todo lo que he mencionado a lo largo de este artículo. La mayoría de los riesgos que tienen los dispositivos conectados

a internet, es decir, los dispositivos IoT está relacionado con la seguridad. Estos riesgos no surgen únicamente por el desconocimiento de los usuarios finales. Los fabricantes muchas veces tampoco dan lo mejor de si para que estos dispositivos tengan el menor número de brechas de seguridad. A su vez, como he mencionado a lo largo de este post, tanto los dispositivos personales como los empresariales están comprometidos, y muchas veces no es necesario contar con un gran nivel de conocimiento para poder aprovechar dichas brechas de seguridad. En el área empresarial, que creo que es la que más perdidas puede generar, ISACA menciona 3 áreas de riesgo para tener en cuenta: el área operacional, el área financiera y el área técnica [5]. Finalmente, aunque estas áreas de riesgo me parecen un tema muy interesante, no voy a profundizar en las mismas en este post.

Bibliografía

[1] <<Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations>>, Oceano, consultado el 20/11//2020, https://ieeexplore-ieee-org.proxy-oceano.deusto.es/document/8688434

[2] <<7 biggest IoT risks facing businesses today – and what to do about them>>, TechGenix, consultado el 20/11/2020, http://techgenix.com/biggest-iot-risks/

[3] <<Breaking Down Mirai: An IoT DDoS Botnet Analysis>>, Imperva, consultado el 20/11/2020, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[4] <<Threat Intelligence Report Says IoT Attacks Doubled Within a Year, Predicts an Upward Trend>>, CPO magazine, consultado el 20/11/2020, https://www.cpomagazine.com/cyber-security/threat-intelligence-report-says-iot-attacks-doubled-within-a-year-predicts-an-

upward-trend/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Threat+Intelligence+Report+Says+IoT+Attacks+Doubled+Within+a+Year%2C+Predicts+an+Upward+Trend&utm_campaign=Weekly+Highlights

[5] <<Internet of Things: Risk and Value Considerations>>, ISACA, consultado el 20/11/2020, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpiot