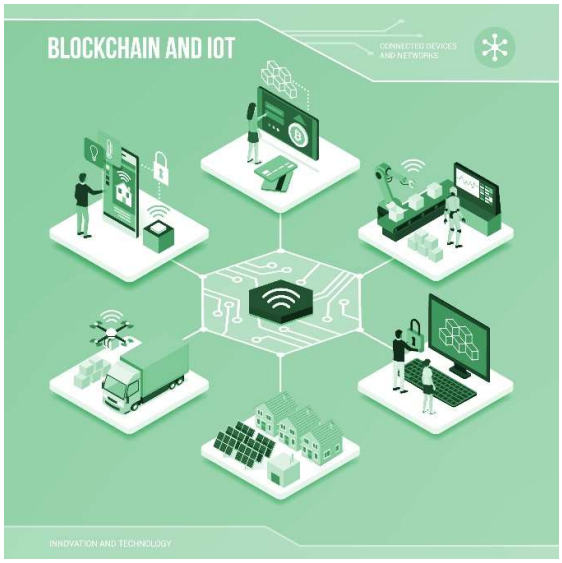
Tendencias de PKI & IoT

- La influencia del IoT y las nuevas aplicaciones han impulsado el uso de la tecnología de PKI. El IoT o Internet de las Cosas se está convirtiendo en un importante motor para el uso de la PKI, al ser su tecnología central para la autenticación.

- En los próximos dos años, el 42% de los dispositivos de IoT dependerá de los certificados digitales para la identificación y autenticación.

- Principales amenazas del IoT: Alterar la función del dispositivo (malware); Controlar el dispositivo de manera remota; Captar datos internos; Usarlo como punto de acceso a una red.



- Proteger la confidencialidad y la integridad de los datos del dispositivo es la capacidad de seguridad del IoT más importante hoy en día.
- Tendencias en la madurez de la PKI: Los módulos de seguridad de hardware (HSM) son el método usado con mayor frecuencia, debido a su seguridad, para la administración de claves privadas para las entidades de certificación de raíz/políticas/emisiones. El uso de HSMs para administrar llaves privadas aumentó un 3% desde 2018 hasta un 42%.

- El 42% de las organizaciones participantes en este estudio que usa los HSMs para proteger la PKI indica que utiliza estos módulos en toda la arquitectura de esta Infraestructura de Clave Pública.

- Como ejemplo de buena práctica, el Instituto Nacional de Estándares y Tecnología (NIST) insta a “Garantizar que los módulos criptográficos para las entidades de certificación (CA), los servidores de recuperación de llaves y los servidores OCSP sean módulos de hardware validados que cuenten con la certificación FIPS 140-2 Nivel 3 o superior”; sin embargo, solo el 11% de los encuestados indica la presencia de HSM en sus instalaciones de OCSP. Esta es una brecha considerable entre las buenas prácticas y las prácticas observadas.

- A menudo, resulta difícil que las aplicaciones utilicen la PKI, entre los mayores desafíos encontramos: La PKI actual no es compatible con nuevas aplicaciones, no tiene capacidad para cambiar aplicaciones antiguas y sus habilidades y recursos son insuficientes.

- Tendencias respecto de los desafíos de la PKI: Las organizaciones con CA internas usan un promedio de ocho CA de emisión independientes que gestionan un promedio de 38.631 certificados obtenidos interna o externamente.

- La PKI es el factor primordial de la red informática de la empresa. No solamente la cantidad de aplicaciones que dependen de la PKI, sino su naturaleza indica que la PKI es una parte estratégica de la red informática principal. Un promedio de 8,5 aplicaciones y certificaciones son administradas por la PKI.

- El principal problema para la implementación de una PKI es que no queda claro quién es responsable por la función de la PKI, también conocida como Infraestructura de Clave Pública.

- Common Criteria EAL Nivel 4+ es la certificación en materia de seguridad más importante cuando se trata de implementar la infraestructura de una PKI y aplicaciones basadas en una PKI. El 66% afirma que Common Criteria es la certificación más importante al implementar una PKI, seguido por el 60% que menciona la FIPS 140.

- Las redes privadas, las redes privadas virtuales (VPN) y las aplicaciones y los servicios basados en la nube incrementan significativamente el uso de credenciales de PKI: Las aplicaciones que utilizan, con mayor frecuencia, las credenciales de PKI son los certificados SSL para sitios web y servicios públicos.

- Otras aplicaciones y servicios que se usan principalmente son las redes privadas y VPN junto con las aplicaciones y servicios basados en la nube pública, la seguridad en el correo electrónico y las autenticaciones de usuarios de la empresa.

- Estos son los componentes básicos de un sistema informático empresarial moderno y los certificados digitales se han convertido en algo parecido al almacenamiento, un componente básico del sistema, que ya no es un complemento exótico.

¿Cuáles son los métodos más populares para implementar la PKI empresarial?

- El método más citado para implementar una PKI empresarial se realiza mediante un servicio gestionado por una entidad de certificación (CA) corporativa interna o uno gestionado por una CA privada externa.