**Las diferencia en Seguridad informática de IaaS, PaaS, y SaaS**

Software as a Service (SaaS) Yo voy a tener una aplicación completamente instalada ya en el proveedor en donde la plataforma y la infraestructura de detrás me lo va a brindar el proveedor. Qué significa esto que yo no voy a tener ninguna opción de elegir qué tipo de equipamiento se va a instalar qué tipo de sistema operativo se va a instalar qué tipo de lenguaje de programación qué tipo de API etcétera.

Lo único que voy a poder hacer es consumir la aplicación a través de un navegador o a través de una aplicación Mobile y en general cuando estoy haciendo un pentest no voy a ver mucho más que un requerimiento tipo get o tipo post que púede ir por http o https o a través de algún otro tipo de canal de comunicación y en general las herramientas para utilizar quizás son lo más cercano a lo que voy a tener a un análisis de un pentest web. Que significa esto, Que como lo único que voy a ver van a ser peticiones del tipo HTTP con sus respectivas cabeceras y demás voy a poder analizar cada uno de los requerimientos y cada una de las respuestas del servidor tratando de encontrar algún tipo de vulnerabilidad que en general como es Software as a Service es algo que va a estar relacionado a esa aplicación o a ese software. Quizás es el más parecido a lo que vamos a encontrar a un pentest tradicional porque lo único que veo efectivamente es una página web o una aplicación móvil.

**Plataforma como servicio en** este caso sí voy a poder seleccionar por ejemplo el tipo de sistema operativo, vamos a ir azure y quizás voy a estar interesado en armar toda una infraestructura de Active Directory con distintos servidores de tipo Windows que obviamente también pueden ser Linux sin ningún tipo de problema. Pero quizás si elegí azure y tecnología Microsoft sea porque me interesa el ambiente Microsoft y en ese caso voy a poder elegir el sistema operativo voy a poder elegir el lenguaje de programación voy a poder elegir el tipo de Apis, el tipo de firewall que quiero instalar etcétera etcétera.

Acá ya empieza a cambiar radicalmente el tipo de pentesting que voy a hacer porque aparte de la página web y el software que yo voy a instalar sobre esa plataforma también voy a poder testear o probar el sistema operativo o los puertos abiertos. Cómo se comunica ese servidor. Qué tipo de protocolos utiliza. Qué tipo de protocolo tengo bloqueados, Cómo instalé el firewall las reglas del firewall , los usuarios, que tipo de permisos tienen esos usuarios. Y acá es donde entran de vuelta lo que mencionaba al principio, de que probablemente por ejemplo si yo tiro un WAF (Web Application Firewell) o un análisis de un WAF o un análisis de un sistema operativo , un nmap por decir algo bien sencillo contra la plataforma. Lo más probable es que voy a terminar viendo lo que el servidor de cloud me quiera mostrar. Por qué?. Porque más allá de que yo instalé mi propia plataforma dentro del servidor de Cloud en realidad estoy pasando por un filtro de ese proveedor.

Qué significa que si yo dejé el puerto 21. abierto por ejemplo porque era mi intención dejar el FTP abierto. Probablemente por algún comunicado interno por un análisis interno en realidad y una auditoría interna del servicio de Amazon de ayuda etcétera de cloud en general me va a informar que no es recomendable tener el 21 abierto y me va a informar una vez me va a informar dos veces y a la tercera me lo va a cerrar. Entonces en ese caso ya están funcionando un montón de análisis adicionales que el mismo proveedor de cloud me ofrece y por lo tanto mi nivel de seguridad inmediatamente ya creció más de lo que estaba. Lo que sería en una plataforma por ejemplo onpremis que nadie me iba a avisar si tengo el 21 abierto me voy a enterar cuando alguien me ataque de última o porque haya alguien realizado un pentest tradicional y me haya avisado.

Y finalmente voy a tener la infraestructura como servicio en donde ya directamente voy a poder elegir completamente qué tipo de computadora quiero cuánta memoria qué tipo de red tengo si voy a instalar equipos de tipo appliance algún tipo de firewall que lo puedo configurar físicamente entre comillas pero en realidad es virtual esto también es un juego de palabras pero es así yo puedo comprar un F5 por decir algo una marca conocida y muy cara una en la nube totalmente virtualizado y a partir de ahí es exactamente lo mismo que si yo tuviera la cajita en la mano es exactamente igual. a partir de ello voy a poder configurar completamente toda la plataforma de hardware en la nube. Exactamente lo mismo que si hubiera comprado el equipamiento pero en vez de comprar lo físico lo compro virtual

Entonces estas serían las diferencias radicales digamos que existe entre un entorno normal y algo Cloud.