Architecture Implementation

Transcribed on July 25, 2025 at 4:15 PM by Minutes AI

Speaker 1 (00:00)

La solución del ejercicio propuesto anteriormente, que hemos resuelto con el Microsoft Threat Modeling.

En este vídeo explicaremos paso a paso toda la implementación de la arquitectura que propusimos en el anterior ejercicio, punto por punto, desde los elementos a las conexiones e incluso a la ejecución de los informes.

Bien, he puesto ahí abajo a la izquierda ese croquis que hemos hecho a mano para tener una referencia y saber lo que tenemos que ir construyendo.

Comenzaremos por lo primero, que es la máquina virtual, que es el servidor, pues directamente aquí en stencils, que son los elementos que realmente tenemos que manipular, porque ahora veremos que hacerlo nosotros a mano directamente puede ser un poco lioso porque tenemos que crear muchos parámetros, en cambio si utilizamos un stencil ya creado, ya viene por defecto con muchísima información, entonces yo aquí pondría directamente virtual y ya aparecerá aquí, ¿Lo veis?

Virtual machine, pues cojo y la arrastro hacia esta zona.

Ya tenemos aquí el primer elemento que era la máquina virtual.

Los dos elementos que nos faltan son las bases de datos, con lo cual si nos vamos aquí y ponemos y aparecerá un listado de todas las que tenemos, en este caso tenemos la que es local, que la que está en la red interna, que es la SQL Database, pues directamente la ponemos y la colocamos aquí cerca, tenemos dos elementos y ya por último nos faltaría nuestro cloud storage, que poniendo cloud directamente ya nos aparece el cloud storage directamente aquí y nada, pues lo ponemos también fuera.

En la rejilla tenemos ya los tres elementos que hemos definido, así que el siguiente paso va a ser interconectarlos, con lo cual si venimos aquí y ponemos HTTPs, ya veremos esa conexión del dataflow, la cogemos, la arrastramos y según dijimos en el esquema, esta conexión iría desde la base de datos SQL que irá aquí, hasta la máquina virtual, que la podemos poner aquí.

La siguiente conexión sería desde la máquina virtual hacia la base de datos SQL, pero en este caso era una HTTP, pero ya que tenemos aquí seleccionado el HTTPs, la aprovechamos y la ponemos fuera para hacer la conexión para la conexión entre la máquina virtual y también el aquí el cloud storage.

Bien, pues ya tenemos más o menos las conexiones que teníamos previstas en el esquema de aquí abajo, pero nos falta el HTTP, con lo cual quitamos la s, aquí ya lo vemos, lo arrastramos y ahora pues ponemos la conexión, en este caso sería al revés, sería de aquí hasta la base de datos, algo así.

Bien, como podéis ver es exactamente igual el esquema que hicimos a mano alzada, que podéis ver abajo a la izquierda, con lo cual es muy intuitivo.

Si os fijáis son como poner piezas de diferentes puzles e interconectarlas entre ellas, viendo una relación muy directa entre lo que hemos hecho a mano con lo que vamos a implementar.

Finalmente sólo nos quedaría hacer la separación de la Boundary.

Para ello sólo tenemos que irnos aquí y escribir Boundary.

Sacamos la de Internet y hacemos lo que os marcar toda la secuencia, toda la traza y que corte donde queremos que se active la conexión hacia Internet.

En este caso con esto nos bastaría, algo así estaría bien.

Vale, pues esta es nuestra arquitectura, esta es la implementación directa de lo que hemos hecho en papel, pero ya plasmada en la herramienta de Microsoft de Tool Modeling.

Ya sólo nos quedaría comprobar que todas las conexiones se han hecho correctamente y para eso tenemos esta opción de aquí que pone Diagrama Reader, en el que le pinchamos y si marcamos la opción de Read Full Diagram, lo que va a hacer es comprobar que todas esas conexiones están funcionando bien, que no hemos cometido un error en conectar los puntos de conexión o que nos falta un elemento que no está relacionado con nada directamente.

Al pinchar aquí nos sale como una descripción de cada uno de los elementos y su conexión.

Como podéis ver, incluso aparece la que indica la conexión hacia Internet desde la máquina virtual hasta el servicio en cloud, como podéis ver aquí, que marca como Internet Boundary.

Las otras dos son la HTTP, como podéis ver aquí, y la HTTPs que van desde el servidor hacia el SQL, con lo cual está correcto y nos vale para validar y estar seguros de que ya podemos ir a la fase de informe.

La parte de informe es muy sencilla, simplemente hay que ir aquí a la parte de Reports y marcamos en Create Full Report.

Después marcamos en que en el botón que lo genera nos pedirá un nombre, lo ponemos en el escritorio y le llamamos.

Importamos a guardar.

Bien, este sería el informe del modelado de amenazas, donde deberían de aparecer una serie de posibles problemas de seguridad o incluso vulnerabilidades, o incluso también algún tipo de amenaza genérica que puedan afectar a la arquitectura que hemos diseñado.

Como podéis ver aquí no aparece ninguna información porque yo no he elegido la acción custom, que es la que me permite definir bien todos estos campos y lo que me interesa es la parte de aquí abajo.

Como podéis ver aquí ya nos dice los 12 elementos que ha analizado o que ha chequeado dentro de nuestra arquitectura.

Entonces a partir de este punto lo que va a hacer es ir analizando cada uno de los bloques para contarnos cuáles son las amenazas que se han encontrado dentro de nuestra arquitectura.

De hecho fijaros, se va fijando antes te hace aquí un esquema global que simplemente es la arquitectura, pero aquí ya se va centrando en los diferentes bloques.

Para empezar comienza con la interacción del HTTP, que quizás una de las más inseguras y aquí nos muestra una relación de posibles problemas.

Estos problemas ya lo hemos visto en otros vídeos sobre el trip modeling en el que sobre todo también de OWAS, por ejemplo aquí podemos ver el primero nos dice que puede haber un problema de spoofing, quiere decir que la base de datos se podría interceptar la información, alguien por ejemplo un man in the middle en el centro de la conexión y modificar esos datos que van de un sitio a otro, esto por supuesto es un problema muy grande porque sería una alteración de la información.

Después tenemos que también podría haber algún tipo de fallo de seguridad, por ejemplo una muy directa sería un tampering, que sería el punto número 2 que veis ahí, que sería un ataque simple de SQL Injection por ejemplo.

Y ya también el tercer punto, más que un ataque también nos está avisando de que aparte de que por supuesto un ataque de deterioración de servicio de muchas llamadas a la vez al servicio podría pararlo, podría parar la arquitectura, pero también tenéis que tener en cuenta que un ataque de denegación de servicio también se puede provocar internamente, si no hay una buena configuración del servidor o de la base de datos, es posible que esa máquina no funcione bien y llegue incluso a generar un auto denial of service, un auto, eso también es un problema de seguridad.

Y bien pues aquí ya iría continuando con todo el informe, si bajamos un poco pasaría a la parte HTTPs, aquí veis que solamente hay dos posibles problemas y también la conexión hacia Internet, que esta es la que posiblemente más fallos de seguridad nos puede ofrecer.

Fijaros que hay más información sobre posibles amenazas porque tiene sentido es la conexión que va desde la máquina que está en la intranet o en la red local hacia Internet, por ese motivo tiene muchas más posibilidades de que sufra algún tipo de problema de seguridad.

En resumen, el ejercicio que hemos concluido resalta la efectividad de la herramienta de modelado de amenazas de Microsoft para fortalecer la seguridad de nuestra arquitectura.

Aquí podemos comprender la importancia que tiene las medidas de seguridad preventivas y además también aprender a aplicar diferentes técnicas de modelado de amenazas de una manera práctica, pero sobre todo sencilla, rápida y también escalable, porque esto nos permite identificar y abordar fallos de seguridad, mejorando la resiliencia de nuestros sistemas frente a las grandes amenazas cibernéticas o a las amenazas de ciberseguridad.

Llegamos al final de la sesión, os esperamos en el siguiente.