Objetivo no viable

MARCO TEORÍCO

2018

ABSTRACT

Un sistema, una organización o un determinado activo se considera seguro si es capaz de defenderse de todos los ataques posibles, incluyendo los ataques que son desconocidos para el defensor.

Las organizaciones, que cuentan con recursos limitados para defenderse, normalmente desarrollan defensas sólo para aquellos tipos de ataques que conocen, por lo que es muy probable que nuevos tipos de ataque, tengan éxito.

La alternativa obvia, es construir las defensas de un sistema en base a una serie de principios o paradigmas básicos que cumplan las siguientes especificaciones:

La validez de los principios debe transcender a tecnologías y ataques específicos

Deben ser aplicables en entornos reales

Deben introducir nuevos modelos y abstracciones que aporten valor pedagógico y predictivo

Permiten describir relaciones no obvias entre ataques, defensas y políticas, de forma que proporcionen una mejor comprensión del panorama general de la ciberseguridad

El desarrollo de dichos paradigmas o leyes generales debe ir más allá de la búsqueda de vulnerabilidades en los sistemas ya implantados y más allá de buscar defensas para ataques específicos.

El paradigma que desarrollamos más adelante (Objetivo No Viable) cumple con las anteriores especificaciones, puesto que va a relacionar los recursos limitados de la defensa, con los recursos limitados del atacante. Estableciendo una abstracción, generalizando los sistemas que son objetivos potenciales para un atacante en función del valor que el mismo asigna a un grupo de sistemas.

Además, utilizando la seguridad ofensiva como hilo conductor para el cálculo de probabilidades, es posible en muchas situaciones inferir o predecir los posibles nuevos tipos y técnicas de ataque utilizadas, anticipando la defensa al ataque.

INTRODUCCIÓN

La seguridad de la información siempre ha sido una de las grandes preocupaciones de las empresas. La protección de los activos, tanto físicos como lógicos, es actualmente de gran importancia para el ejercicio de cualquier actividad, y necesita de nuevas medidas de seguridad y metodologías para acometer los retos que supone.

Actualmente esta protección se basa siempre en supuestos teóricos que llevan, por un lado, a un sobrecoste en la implantación de medidas de seguridad, como a la falta por completo de ellas, debido precisamente al coste necesario de abordar toda la infraestructura IT de una organización.

A lo largo del tiempo se han realizado estudios teóricos intentado predecir tanto la probabilidad como la periodicidad de los ataques informáticos sobre la infraestructura IT de una organización. De estos estudios se desprende que de alguna manera es posible predecir, de manera más o menos precisa, cuándo una organización sufrirá un incidente de seguridad, y en qué manera le afectará.

En este estudio, se detallarán las partes involucradas en un incidente de seguridad, a la vez que desarrollaremos el marco teórico sobre el que se sustenta el Objetivo No Viable.

Esta metodología, lejos de intentar proteger toda la infraestructura de IT de una organización, tiene su fundamento en la criticidad de los componentes, actuando sobre aquellos fundamentales para el funcionamiento del modelo de negocio de una organización, así como para la continuidad en el tiempo del mismo.

Para su desarrollo, esta metodología recoge conceptos sobre acciones y tácticas más relacionadas con otros ámbitos como el coste de un ataque, o los recursos consumidos y necesarios para llevarlo a cabo.

MARCO ACTUAL

La coyuntura actual respecto de la seguridad de la información nos sitúa dentro de un marco de incertidumbre respecto de las acciones a tomar para proteger la información. Esto se comprueba en los siguientes gráficos:

Como se puede comprobar, la inversión en ciberseguridad aumenta año a año. Este hecho debería resultar en una disminución de los incidentes de seguridad, pero no es así:

Por lo tanto, la coyuntura de incertidumbre se acrecienta, al comprobar cómo los incidentes de seguridad reportados aumentan, pese al aumento de la inversión en ciberseguridad.

Esto lleva a la conclusión inmediata de que la seguridad de la información podría abordarse de alguna otra manera, en la que el Retorno de la Inversión en Seguridad (ROSI por sus siglas en inglés) sea apropiado en la función:

$$\frac{\Delta\ Número\ incidentes\ de\ seguridad}{\Delta\ Inversión}$$

El comportamiento esperado de esta función es que año a año, descienda el número de incidentes de seguridad por cada euro invertido en seguridad, y a la luz de los resultados, se comprueba que esto no es así.

Además, las predicciones auguran un aumento de estos incidentes, lo que todavía agrava más la situación. A su vez, se constata que los atacantes son individuos u organizaciones cada vez más decididos y profesionalizados.

Llegados a este punto, la pregunta que debemos hacernos es: ¿Qué podemos hacer para cambiar esta tendencia?

PROBABILIDAD DE SUFRIR UN ATAQUE INFORMÁTICO

El primer paso, fundamental para la metodología del Objetivo No Viable, es medir de la manera más precisa posible la probabilidad de sufrir un ataque informático exitoso. La cuestión crítica en este caso es ¿exitoso respecto a qué?

Por norma, se tiende a realizar estudios estadísticos respecto de todo el sistema de gestión de la información y telecomunicaciones. Esto en muchos casos supone un grandísimo coste en términos de inversión y mantenimiento de la infraestructura y comprobación de las medidas de seguridad desplegadas. Y a la luz de los resultados de los estudios sobre el número de incidentes de seguridad, se está comprobando que no es un acercamiento eficaz.

Por eso, es crítico identificar la infraestructura sobre la que se va a medir la probabilidad de recibir un ataque exitoso. [3]

Enfrentar la probabilidad de recibir un ataque, utilizando las tablas de evaluación de riesgos, no da una métrica válida para determinar la probabilidad de sufrir un ataque exitoso el cuál, además, reporte un beneficio para el atacante.

Esto se debe a que los tipos de ataque que se pueden recibir son numerosos, y la pretensión de cada uno de ellos es diferente.

Además, muchos de los ataques serán detenidos por las defensas perimetrales, los cuales no llegarán a convertirse en una amenaza real.

Una vez identificado el activo crítico, el cual se quiere proteger, hay que medir esta probabilidad. Para obtener un resultado preciso, existe una herramienta que da un valor con una gran certeza, los test de intrusión.

TEST DE INTRUSIÓN

Consiste en simular un ataque informático, utilizando las herramientas y la metodología de un atacante, para comprobar de manera fehaciente la capacidad de defensa de un sistema informático, además de otros parámetros como el grado de acceso, la capacidad de detección o incluso la capacidad de recuperación del sistema.

Dentro de la batería de test a realizar se obtienen resultados de:

-Nivel de exposición

-Facilidad de acceso

-Tecnologías en uso

-Grado de explotabilidad

-Grado de accesibilidad de información

-Protección ante ingeniería social

El resultado de usabilidad de los resultados de estas pruebas, siempre estarán supeditados al sistema comprobado. Es por este motivo que identificar el activo crítico para la organización es clave para tomar por válidos estos resultados.

ACTIVO CRÍTICO

Para que el cálculo sea lo más correcto posible, la empresa, con anterioridad al test, debe identificar de manera clara cuál es el activo más importante, el que debe proteger. O por lo menos, el activo que tiene el beneficio potencial más alto para un posible atacante.

Gracias a esta determinación anterior a la realización del test, se puede comprobar de manera precisa la probabilidad de éxito de un atacante, y por lo tanto, se puede inferir de manera directa la probabilidad de sufrir un ataque.

Esta probabilidad también se verá afectada por las motivaciones del atacante.

MOTIVACIONES PARA EL ATACANTE

El primer punto, necesario para el desarrollo del Objetivo No Viable es modificar el KillChain de un ataque informático para introducir un paso más, la motivación para realizarlo.

Este punto es muy importante, ya que en función de la motivación que se tenga para llevar a cabo un ataque informático el coste del mismo para el atacante, o el beneficio que perciba será diferente, y, por lo tanto, las medidas a tomar también diferirán.

Los ataques informáticos se pueden dividir en tres grandes grupos:

ATAQUES GENERADOS DE FORMA AUTOMÁTICA

Este tipo de ataques se pueden definir como "la caza del objetivo más fácil". Aunque se producen de manera constante, alcanzan picos de actividad que pueden ser muy peligrosos cuando se hace público un *exploit* para una vulnerabilidad de tipo *Zero Day*. Durante el tiempo que transcurre entre la publicación del *exploit* y la publicación del parche de seguridad o remedio que lo palia, se generan multitud de ataques automatizados en busca de equipos que tengan esta vulnerabilidad.

En este caso la relación entre coste/beneficio es tan baja, que el coste se puede considerar prácticamente cero. Es decir, llevar a cabo este tipo de acciones, resulta para el atacante siempre beneficioso, por lo que hay que contar con que se van a producir.

Por contra, la solución a este problema de seguridad, también lleva aparejado un coste muy bajo. Generalmente, como ya se ha comentado, en forma de aplicar un parche de seguridad, o modificar la configuración insegura que sirve para explotar la vulnerabilidad.

ATAQUES SIN MOTIVACIÓN ECONÓMICA

En el otro extremo de la balanza entre coste y beneficio se encuentran los ataques realizados por motivos sin motivación económica, como pueden ser:

-Hacktivismo

-Venganza

-Terrorismo

-Guerra de la información

-Inteligencia/Contrainteligencia

Estos ataques tienen como finalidad causar un daño directo a la empresa, sin esperar el atacante un beneficio económico directo por sus acciones. Por lo tanto, como este ataque se basa en causas irracionales, no se va a poder evitar por el mero hecho de no resultar beneficioso económicamente para el que lo perpetra.

ATAQUES DIRIGIDOS

Los ataques más habituales son aquellos dirigidos contra una organización en concreto. Además, el atacante en este caso, sí tiene motivaciones económicas y busca constantemente la relación coste/beneficio de manera que sea rentable para él.

La planificación de estos ataques, generalmente consume una gran cantidad de tiempo, puesto que el atacante busca la manera más sencilla y eficaz de conseguir el objetivo propuesto. Sufrirlos, por otra parte, conlleva un impacto económico fuerte para la organización.

En muchas publicaciones se ha establecido que, en la cadena de evaluación de riesgos, si el coste del ataque es superior al beneficio obtenido se puede asumir el riesgo, puesto que el atacante no iba a realizar ese ataque por no ser viable.

Basándonos en esta presunción, hemos intentado desarrollar este planteamiento, para darnos cuenta de que, en lugar de evaluar cada amenaza concreta, deberíamos evaluar el sistema por completo bajo este prisma, buscando todos los posibles vectores de ataque hacia el objetivo.

Inmediatamente surgen varios problemas, el primero es el de calcular el coste de un ataque, de manera casi instantánea se comprueba que esta métrica es totalmente imposible de cuantificar, puesto que los parámetros que intervendrían en su cálculo son demasiado complejos, puesto que habrá atacantes que tomen como referencia el tiempo que les cueste llevar a término un ataque, por el contrario, otros tendrán como prioridad el coste monetario de realizarlo (software, hardware, dispositivos de apoyo, etc...)

Además, también habría que establecer una escala dentro de las habilidades de cada atacante, sumando esta al cómputo global del coste, ya que un atacante experimentado que ya posea los recursos materiales necesarios para llevar a cabo el ataque, tendrá un coste más bajo que el inexperto o carente de los recursos materiales iniciales para realizar el ataque.

Pero además de esto, el siguiente problema aparece al intentar medir el beneficio. Es decir, cuánto vale el activo que se quiere proteger, desde el punto de vista del atacante.

Es evidente que, para el propietario de este activo, el valor será mucho mayor que para el atacante, es decir, hay una discrepancia en el valor percibido, a la hora de calcular el beneficio resultante de llevar a cabo el ataque.

Por lo tanto estamos tratando con dos magnitudes que no son determinables de forma objetiva como son:

- el coste que el atacante debe pagar para llevar a cabo el ataque
- el valor que el atacante asigna al éxito del ataque, es decir el beneficio que el atacante espera por alcanzar los objetivos del ataque.

Este planteamiento es cierto para cada sistema de manera individual.

Sin embargo, podemos hacer la siguiente abstracción: el sistema que queremos defender, no es un sistema aislado, sino que comparte espacio con una infinidad de sistemas similares (similares desde el punto de vista del atacante, puesto que, el beneficio que obtendrá de cualquiera de ellos será similar, con un coste de ataque equivalente).

COSTE DE OPORTUNIDAD

Actualmente en el mundo existen millones de sistemas, de ellos, cientos de miles forman parte de los activos críticos de las empresas.

Dentro de estos cientos de miles, existen sistemas más o menos vulnerables, para los cuales la probabilidad de sufrir un ataque exitoso es medible de manera precisa, como ya se ha visto y, además, existen sistemas muy similares entre ellos.

Por lo tanto, no debemos valorar lo que cuesta vulnerar un sistema concreto, sino lo que cuesta vulnerar, de MEDIA, a cualquiera de los sistemas similares a él. Dicha media, no es más que una percepción totalmente subjetiva, de hecho cada atacante puede asignar un valor distinto a dicha media.

Sin embargo, cuando un atacante decide actuar de forma lógica y con la intención de obtener un rendimiento económico contra un sistema, elige entre aquellos que cumplan las siguientes condiciones:

-El ataque se lleve a cabo de manera exitosa con gran probabilidad, es decir que el ataque sea factible.

-El ataque no cueste más de lo que costaría realizarlo contra un objetivo similar, es decir que no haya pérdida en coste de oportunidad.

Si cualquiera de las dos condiciones no se cumple en un sistema concreto, el atacante tiene inmediatamente una pérdida en términos de COSTE DE OPORTUNIDAD, vulnerando o intentando vulnerar el sistema objetivo.

Es decir, si el atacante percibe que la probabilidad de vulnerar un sistema, es inferior a la probabilidad de vulnerar uno similar, no lo atacará, porque implicaría un beneficio menor, es decir, tendría una pérdida.

Por ejemplo, si un atacante puede vulnerar un sistema en una semana obteniendo un beneficio X, el mismo atacante no atacará a un sistema en el que tenga que invertir 4 semanas para obtener el mismo beneficio, al menos mientras existan otros sistemas similares al primero.

OBJETIVO NO VIABLE

Una vez que hemos introducido todos los conceptos y datos anteriores, podemos ya definir de manera precisa el Objetivo No Viable:

El paradigma de la defensa convirtiendo a un objetivo en no viable, establece que:

"En el caso de ataques dirigidos, el atacante debe invertir una serie de recursos para llevar a cabo el ataque, además el éxito del ataque tiene una probabilidad p, obteniendo un beneficio en caso de éxito. Por lo tanto la lógica para llevar a cabo un ataque se reduce a tener en cuenta la esperanza matemática de la variable aleatoria X que describe el ataque":

$$E[X] = Bp - I(1-p)$$

Donde B representa el beneficio que recibirá el atacante en caso de éxito, I es la inversión en recursos que el atacante debe realizar para llevar a cabo el ataque, independientemente del éxito o fracaso del mismo.

Ahora bien, el beneficio B puede ser expresado en función de la recompensa total, R, que el atacante reciba como resultado del ataque exitoso, menos la inversión, I, que ha realizado para llevar a cabo el ataque $(B = R - I)$:

$$E[X] = (R-I)p - I(1-p)$$

$$E[X] = Rp - Ip - I + Ip$$

$$E[X] = Rp - I$$

Donde R representa la recompensa total obtenida como resultado del éxito del ataque. Esta recompensa, se cuantifica como se ha visto anteriormente en término de coste de oportunidad, por lo que podemos asignar el valor 1.

Esto significa que, desde el punto de vista del atacante, resulta rentable llevar a cabo el ataque, únicamente en el caso en el que $E[X] \geq 0$.

En caso contrario el ataque supondría pérdidas para el atacante, convirtiendo al objetivo en no viable para el ataque.

Ahora bien, como ya se ha explicado, tanto la inversión a realizar por el atacante, como el coste del ataque, como el valor percibido por el atacante no es posible de calcular. Pero tampoco es necesario su cálculo, puesto que, asumiendo que existen dos sistemas que ofrecen la misma recompensa por la misma inversión, tendremos que:

$$E_1[X] = Rp_1 - I$$

$$E_2[X] = Rp_2 - I$$

Donde $E_1[X]$ es el beneficio esperado por atacar al objetivo 1, mientras que $E_2[X]$ es el valor esperado por atacar al objetivo 2, de tal forma que, siendo $p_1 < p_2$ el atacante tendrá una perdida en forma de coste de oportunidad dada por

$$Perdida = R(p_2 - p_1)$$

Es decir, la pérdida es de un $(p_2 - p_1)$ % del beneficio que se obtendría por atacar a un sistema con una probabilidad mayor de éxito. Por tanto el Objetivo 1 es un objetivo no viable para el atacante.

Resulta evidente que la organización, no puede reducir de forma unilateral la recompensa que el atacante percibe que puede obtener por vulnerar el sistema, sin embargo, sí que puede reducir la probabilidad de éxito del ataque, lo que va a reducir de forma drástica la cantidad de recursos que el atacante estará dispuesto a consumir para llevar a cabo el ataque, dada la escasa probabilidad de éxito y la pérdida en coste de oportunidad que ello supondría, como acabamos de ver.

Además, dentro de los ataques dirigidos, los ataques potencialmente más peligrosos que son llevados a cabo por atacantes más experimentados, tienen una mayor probabilidad de ser evitados ya que el atacante será consciente de la dificultad de éxito del ataque y es más probable que desista y no se arriesgue a perder recursos, por lo tanto, se produce un importante efecto disuasorio frente a ataques potencialmente muy peligrosos.

Sin embargo, en los ataques motivados por razones no económicas, la recompensa puede o no ser estrictamente económica, también puede venir dada en base a otro tipo de beneficios no medibles, como puede ser la satisfacción personal, los ánimos de revancha, etc… Pero en todo caso el paradigma es exactamente el mismo, el atacante sólo podrá disponer de una cantidad de recursos limitados para llevar a cabo el ataque y una vez superada dicha inversión, se perderá la motivación para llevar a cabo el ataque. Sin embargo, este tipo de ataques basados en motivaciones personales, son los más irracionales y la disuasión del atacante puede ser imposible, sin embargo, asegurando la superficie de la infraestructura crítica y reduciendo la probabilidad de éxito de un ataque contra ella, el potencial atacante, frente a la gran dificultad para satisfacer su deseo de venganza, se verá más motivado a atacar a cualquier otro sistema que resultará menos crítico para la organización.

MANTENIMIENTO DE P

De cara a la defensa, una vez que se ha conseguido establecer una probabilidad de sufrir un ataque inferior a la de los sistemas similares, el objetivo pasa a ser el mantenimiento de esa probabilidad dentro de los niveles que ocasionen una pérdida en términos de coste de oportunidad para el atacante.

El campo de la seguridad de la información, tanto del lado del atacante como del defensor, está en constante cambio y transformación, siendo necesaria la rápida actuación en determinadas circunstancias, y manteniendo un nivel de alerta coherente con el activo que se quiere proteger.

Para mantener la probabilidad de sufrir un ataque exitoso dentro de los niveles de seguridad, hay que acometer una serie de acciones, actuando de manera proactiva sobre el activo que se quiere proteger. Cada una de las acciones tendrá uno de los siguientes impactos en la probabilidad de sufrir un ataque exitoso, *p*:

-**Mantenimiento de *p***: Acciones orientadas a conseguir mantener la probabilidad dentro de los niveles aceptados

-**Reducción de *p***: Acciones que de manera directa o indirecta reducen la probabilidad.

-**Comprobación de *p***: Acciones que devuelven el valor de p actual.

Las acciones concretas para conseguir esto, se extraen de la seguridad ofensiva o hacking ético. Metodología la cual está basada, como ya se ha expuesto, en utilizar las mismas herramientas y métodos que los atacantes:

-Test de intrusión periódicos (**comprobación de *p***)

-Monitorización BBDD de exploits, públicas y privadas (**mantenimiento de *p***)

-Búsqueda de nuevas vulnerabilidades y vectores de ataque (**reducción de *p***)

RESUMEN

Como se ha visto a lo largo del desarrollo, estando en el marco actual debemos realizar acciones que modifiquen las tendencias relativas a incidentes relacionados con la seguridad de la información. Sabiendo que actualmente, las motivaciones de los atacantes son mayoritariamente económicas, resulta evidente que debemos focalizar el planteamiento de la defensa sobre este factor.

La metodología del Objetivo No Viable acerca la postura del atacante con la del defensor, enfrentándolas directamente para obtener al final la relación directa entre las motivaciones iniciales de un ataque, y el resultado del mismo en términos económicos.

Además, gracias a la existencia de herramientas como los Test de Intrusión, es posible calcular el riesgo exacto de sufrir un incidente de seguridad de cualquier tipo en un sistema determinado. Esto permite conocer las mejores medidas de seguridad a implantar para reducir esa probabilidad de sufrir un ataque, de manera que se optimice la inversión en seguridad y se obtenga el máximo ROSI posible.

Por supuesto, las organizaciones deben ser también conscientes de que no sólo es necesario reducir esa probabilidad de manera periódica, sino que la deben mantener lo más baja posible, adoptando las medidas de seguridad apropiadas para esta tarea como son la monitorización constante de sus activos, la implantación de protocolos de seguridad correctos y la revisión constante tanto de las políticas de seguridad como se de aplicación. Este **Ciclo de Vida de la Seguridad de la Información** el cual se orienta principalmente a tomar acción sobre la seguridad, resulta extremadamente efectivo y rentable en términos de protección/inversión.

En conjunto, el Objetivo No Viable es un acercamiento nuevo al diseño, implantación y mantenimiento de la seguridad de la información, con la intención de focalizar los esfuerzos en aquellos activos que resultan indispensables para su funcionamiento o propósito, mientras que se mantiene un moderado nivel de inversión.

Referencias:

[1] https://www.gartner.com/newsroom/id/3836563

[2] www.incibe.es

[3]IEC 62443 – Zones and conduits.

NIST 800-30

OSSTMM V3

CVSS V3.0 - https://www.first.org/cvss/

An Empirical Analysis of Cyber Security Incidents at a Large Organization – Marshall A. Kuypers, Thomas Maillart, Elisabeth Paté-Cornell – Stanford University – UC Berkeley.

Quantifying Information Risk and Security – Ed Gelbsten Ph.D. – ISACA Journal Vol. 4

The Business Model for Information Security – ISACA