UNIVERSIDAD MARIANO GALVEZ DE GUATEMALA

INGENIERIA EN SISTEMAS

INVESTIGACION

Eleazar Obed

Sales Mejia

7691-20-9920

Técnica del salami

Conocida también como estrategia de rebanada de salami, es una estrategia política mediante la cual un grupo es debilitado mediante la segmentación de sus componentes, ya sea mediante amenazad o alianzas de esta forma la oposición es eliminada rodaja, hasta darse cuenta de que ha sido desmantelada por completo.

También pueden incluir la creación de facciones al interior de un grupo opositor, en el las pugnas entre dichas facciones son las que terminan disolviendo al grupo que uso la táctica salami sea visto como culpable.

Aunque inicialmente una estrategia política se usa también en otros ámbitos, aunque con la misma connotación negativa.

La táctica salami surge apenas terminada la segunda guerra mundial hungria, liberada del yugo nazi por las tropas del ejército rojo, se ve ocupada de inmediato por las mismas con la intención de crear un régimen comunista.

Moscu esperaba apoyar a los comunistas húngaros para hacerse con el poder en las primeras elecciones de posguerra, pero estos apenas obtuvieron un 17% del total de los voto.

El partido húngaros que encuadraba a los comuinistas recurrió entonces a la táctica salami.

Alan Bullock y Oliver Stallybrass mencionan en su libro Dictionary of Modern Thought que el término fue acuñado por el dirigente comunista húngaro Mátyás Rákosi, a finales de la década de 1940, con el nombre de szalámitaktika

Rákosi se refería con este término a la estrategia del Partido de los Trabajadores Húngaros para eliminar a los demás partidos rebanándolos como si fueran salami Dicha táctica consistía en acusar a sus rivales más abiertos y audaces de ser simpatizantes fascistas, obligando con ello a los partidos opositores a expulsarlos de sus filas, debilitando con ello sus propias estructuras institucionales. Una vez que los más anticomunistas quedaban fuera, la táctica se repetía con otros grupos, hasta que al final quedaban sólo aquellos abiertos a colaborar con el PCH o que no podían retarlo Una vez debilitados, los partidos opositores desaparecieron, con excepción del Partido Socialdemócrata Húngaro, que se unió al Partido Comunista de Hungría para formar el Partido de los Trabajadores Húngaros en 1948. Este último vendría a establecer la República Popular de Hungría, y gobernar Hungría de 1949 a 1989.

Otros partidos comunistas de Europa Oriental usaron esta misma estrategia.

Durante la Guerra Fría, la táctica salami vino a ser acompañada por otro esquema político llamado «comunismo gulash», también de raíz culinaria y húngara, aunque instaurado por un sucesor de Rákosi, János Kádár.3

Manipulación de los datos de entrada

Un insider es una persona de dentro de una organización que supone un riesgo de seguridad y, por lo tanto, una amenaza interna.

Sus actividades suelen persistir en el tiempo y se producen en todo tipo de entornos: desde empresas privadas hasta organismos gubernamentales, independientemente del tamaño. De hecho, cada vez son más las pequeñas compañías las que están recibiendo este tipo de ataques debido a la creencia que estas suelen tener en materia de ciberseguridad.

No en vano, en términos globales, hasta el 85 por ciento de las organizaciones recibe ataques de manera interna, según datos de McAfee.

No obstante, cabe destacar que todo esto no significa que el actor malicioso sea un empleado de la organización. Puede ser un consultor, un antiguo trabajador, un socio comercial o un miembro del consejo de administración. Eso sí, el nexo común entre todos ellos es que tienen acceso a información privilegiada.

Tipos de insider

Los tipos de insider o de amenazas internas pueden ser varios:

- Una persona con información privilegiada maliciosa que abusa de las credenciales legítimas para robar información por incentivos financieros o personales.
- Un insider descuidado, es decir, aquel que, sin saberlo, expone el sistema a amenazas externas (este suele ser el tipo más común de amenaza interna).
- Un topo o impostor, el cual ha conseguido obtener acceso interno a una red y suele hacerse pasar por un empleado o socio para ganarse la confianza.

Las medidas de detección y protección básicas ayudan a que las organizaciones no sufran la actividad de un posible insider. Algunas de estas recomendaciones de ciberseguridad son las siguientes:

- Utilizar un software de detección de anomalías en la red.
- Restringir el acceso y privilegios según la escala laboral.
- Monitorizar la actividad de los empleados o correos electrónicos para saber dónde se encuentra la información.
- Educar y concienciar a los empleados para que sean capaces de reconocer y evitar los actores maliciosos.
- Contar con personal especializado en ciberseguridad.

Manipulación de los datos de salida outsiders

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Técnica de "ping-pong"

Si ya profundizaste al menos un poco en el mundo de los ordenadores o incluso sueles pasar un tiempo en juegos en línea, el término «ping» seguramente te habrá llamado la atención alguna vez.

Pero el hecho es que, aunque el ping es un viejo conocido para quien suele tener acceso a internet, muchas personas no tienen ni idea de qué es o para qué sirve. Por eso, en Profesional Review, hemos preparado una pequeña explicación sobre el tema.

Qué es el ping

Antes de hacerse conocido como 'ping', este era un acrónimo de Packet Internet Groper, o «Buscador de Paquetes en Redes», en una traducción simple.
Presente en prácticamente todas las redes y sistemas operativos, se trata de un sistema que envía un conjunto pequeño de datos a máquinas conectadas a una red y calcula el tiempo que lleva recibir y responder a esta.
Además de la existencia de un dispositivo conectado a la red, el resultado de un ping también permite obtener información sobre la calidad de la transmisión de datos, principalmente sobre la latencia.

El concepto, aquí, se refiere al tiempo entre el envío del paquete de datos y la recepción de la respuesta. Cuanto mayor es, en milisegundos, más difícil se hace la sincronización de datos en tiempo real.
Se podría hacer un analogismo con el ping-pong. Si los términos técnicos son demasiado para ti, imaginar este deporte es la manera correcta de entenderlo. Por ejemplo, la pelota de ping-pong serían los datos. Mientras que de un lado está el remitente, y del otro el destinatario. Mientras la pelota de ping-pong va de un lado a otro de la mesa, todo marcha bien. Y si el juego se lleva a cabo de manera muy veloz, mejor será la salud de la red.

El ping permite saber si un ordenador remoto está accesible o no (descartando los firewalls).

El comando ping utiliza el protocolo ICMP (protocolo de mensajes de control de red) mediante el envío de un paquete específico para una determinada máquina y espera por la respuesta para registrar el delay. Este delay es denominado 'latencia'.

Para qué sirve el ping

El comando Ping se utiliza a menudo para probar la conectividad IP entre los equipos. Su funcionamiento consiste en enviar paquetes ICMP a un equipo de destino y esperar una respuesta que permita comprobar si el equipo de destino está o no activo, si existe pérdida de paquetes y el tiempo que se tarda en recibir la respuesta.
Antes de todo, es bueno dejar algo claro que Michael Muuss, el creador del sistema, afirmó en su web que su objetivo al dar este nombre era, en realidad, hacer una analogía con el sonido de un sonar (sound navigation and ranging), en el que el ping emite "ecos" a un servidor, y después espera la respuesta.
El motivo de esta analogía procede del hecho de que el comando ping actúa de forma similar a un sonar; sin embargo, con foco en el mundo virtual.
De forma simple, cuanto menor es el valor que se obtiene al hacer ping, más rápida es la conexión.

Cómo hacer ping

A pesar de ser un recurso muy utilizado por los administradores de red o expertos, cualquier persona puede realizar una prueba de ping para, por ejemplo, probar la calidad de la propia conexión. El proceso se realiza a partir del Símbolo del Sistema en Windows, o desde la Terminal, en OS X y Linux.
En las máquinas que funcionan con el sistema de Microsoft, basta con abrir el menú Inicio y, en el campo de búsqueda, escribir «cmd» o «Símbolo del Sistema» en la ventana de búsqueda.

En Mac OS X, el camino es acceder a la carpeta de aplicaciones y, después, a la de Utilidades, para seleccionar Terminal. En Linux, el recurso normalmente se encuentra en la carpeta Accesorios o puede ser accedida por el atajo de teclas Ctrl + Alt + T.

Para hacer una prueba, solo tienes que escribir la palabra ping seguida de la dirección URL de un sitio web cuya conexión será puesta a prueba, o bien la dirección IP de una máquina que esté conectada a tu red.
Diversas informaciones en cuanto a la calidad de la conexión se muestran en la pantalla, y el sistema normalmente realizará cuatro envíos de datos para medir los resultados. En consecuencia, surge el análisis y los números que indican la calidad de la red y la velocidad de transmisión.

Técnica de ECaballo de Toya

En muchas empresas la innovación se ve como algo demasiado complejo de desarrollar y que requiere ingentes recursos para poder obtener un producto o un servicio que sea innovador y genere beneficios.

Frente a este paradigma, una de las opciones que tenemos para cambiar esta visión es utilizar un "Caballo de Troya", es decir, introducir la innovación en la empresa de una forma sutil y sin que se den cuenta los “de dentro” hasta que ya sea demasiado tarde para oponerse a ella.

Esta forma de actuar se apoya en una estrategia para el cambio basada en que “un cambio de comportamiento en una organización es más eficaz si se hacen primero cambios simples en lugar de pretender implementar grandes programas para el cambio”.

Es habitual que los grandes cambios generen grandes resistencias porque suponen modificar la “zona de confort” de las personas; y la introducción de una cultura de la innovación de forma brusca supone para muchas personas que se les ponga en cuestión la forma en que realizan su trabajo o que vislumbren cambios que les hará que tengan que aprender cosas nuevas.

En este caso la estrategia está muy clara pero lo que requiere de un uso avanzado del ingenio será la forma en que introduciremos el "Caballo de Troya" en la empresa.

Lo primero a considerar es si debemos construir un caballo o más de uno; lo más adecuado es preparar una batería de caballos que iremos lanzando de forma sucesiva porque no siempre el primero obtiene el resultado esperado.

Así, por ejemplo, se pueden empezar a desarrollar pequeños proyectos para innovar en los productos, los servicios y especialmente en los procesos; esto último es una de las vías de entrada de los caballos de Troya con más posibilidades porque en las organizaciones en las que no se innova hay muchos procesos que se pueden mejorar introduciendo pequeñas innovaciones, lo que se conoce como "innovaciones incrementales" y que suponen una fuente de incrementos de productividad y competitividad muy importante.

Pero, además, la estrategia del "Caballo de Troya" también es útil cuando se quieren introducir innovaciones tecnológicas disruptivas en productos o servicios porque las podemos introducir como complementos para que los usuarios validen su utilidad.

Esto es útil porque las tecnologías disruptivas no siempre son bien recibidas por los clientes y usuarios ya que suponen cambios relevantes sobre a lo que hasta el momento estaban acostumbrados. Así cuando una innovación disruptiva forma parte del producto al que los clientes y usuarios están acostumbrados es más fácil que la acepten que si se introduce de forma aislada como producto nuevo y diferencial.

Una de las metodologías que podríamos considerar se basa en una estrategia de "Caballo de Troya" es la que se conoce como "gamificación", esta metodología que se basa en el uso de técnicas y dinámicas propias de los juegos y el ocio para aplicarlas a actividades no recreativas entre las que podemos encontrar las relacionadas con el marketing de fidelización o la adopción de nuevas prácticas por parte de los empleados. En este caso el juego es lo que se utiliza como "Caballo de Troya" para conseguir que los clientes o empleados hagan lo que queremos que hagan y así nosotros consigamos nuestro objetivo.