>> Jorge Dávila

¿Cómo medir lo que no ocurre?

En unos tiempos en los que la austeridad reina y en los que hay que justificar hasta los últimos céntimos la conveniencia de un gasto que no sea financiero, la necesidad de justificar la seguridad lógica nos lleva a rendir cuentas de alguna forma pero... ¿cómo se pueden medir los efectos reales de una seguridad que funciona? ¿Cómo se miden los efectos de los desastres? ¿Hay indicadores que podrían explicar lo muy provechoso de mis esfuerzos en defensa digital? No siempre es fácil justificarse, pero muchas veces hay que hacerlo.

De las llamadas Ciencias Experimentales, sin duda la Física de Altas Energías[1] y la Astronomía observacional[2], con sus telescopios[3] de todo tipo, probablemente son "las más caras" de todas. Son muchos los millones de euros que se han fulminado en cada una de esas detonaciones en las entrañas del *Largue Hadron Collider*[4], el mayor de los aceleradores de partículas del mundo, para buscar la mal llamada "*Partícula de Dios*" o *Boson de Higgs*[5]; última *delicatessen* de la Física de Partículas.

Con los vendavales economicistas que hoy soplan, deberíamos considerar esos ejemplos como "*gastos muy caros*", ya que en ellos no hay beneficios inmediatos, ni siquiera tecnológicos, para la población civil que, atónita e inconsciente, los financia. Lo curioso es que, en el caso de la física de altas energías y la astronomía observacional, se da una euforia y complacencia periodística difícil de entender a menos que se analice con el filtro de la religiosidad y el misticismo puesto ante nuestros ojos. En estos casos, tanto la ciencia académica como los periodistas especializados o no, repiten como una letanía *"que los descubrimientos fundamentales tardan décadas en emerger de su esterilidad comercial pero que, cuando lo hacen, suelen cambiar el mundo"*; y la gente, en silencio, lo acepta y sigue pagando.

En realidad, saber cuál es el resultado neto de cualquier tipo de investigación básica es muy difícil de evaluar, de medir. Es prácticamente imposible establecer cuál es el impacto real que tienen las inversiones en ciencia fundamental y básica sobre la vida de los ciudadanos que las costean. También es difícil entender por qué mecanismo la sociedad en general acepta entregar esas cantidades ingentes de recursos a una minoría muy reducida de científicos que hacen de esa comunión con lo eterno, lo esencial y lo inapelable, su forma de vida y su forma de organización gremial.

Esa facilidad de concentración de recursos contrasta con la reluctancia general a la aceptación y financiación de otras actividades más sociales. Otros frentes, menos exitosos, pero que no resultan demasiado mal parados en el reparto de recursos públicos, es el de la seguridad sanitaria, física, alimentaria, etc.; sin embargo, ese no es el caso de la seguridad lógica y la gestión del riesgo como elementos ineludibles en los presentes y futuros sistemas de información.

Es difícil explicar cómo la sociedad tecnológica del siglo XXI se abalanza más y más sobre un sustento funcional esencialmente basado en sistemas de información, y no aplica el mismo ímpetu en la inversión en temas de seguridad lógica, emergencias y gestión del Riesgo.

La economía y la lógica de los mercados rápidamente hablan de la "*rentabilidad*", de la necesidad de conocer qué y cuánto se obtiene a cambio, inmediatamente o en un plazo muy próximo, de toda inversión y, en particular, de las que se hagan en seguridad lógica. Es fácil admitir que el adinerado común esté habituado y entienda de guardias, coches blindados, cajas acorazadas, grilletes y demás parafernalia policial, por lo que no cuestiona en exceso los gastos realizados en esa dirección. Sin embargo, no es tan fácil de entender que ese mismo personaje no se haya dado cuenta ya de que, desde hace tiempo, el valor económico, el dinero, no está asociado a objetos tangibles que pueden ser protegidos con porras y pistolas.

Cuando se consigue llamar la atención sobre la seguridad en los sistemas de información, los directivos siempre terminan planteando si es posible "medir", de alguna forma, lo que se gana invirtiendo en seguridad informática. Solo es esperable la inversión y el reconocimiento de méritos a la seguridad lógica si se obtiene un resultado favorable en esa medida de las ganancias que van asociadas con ella.

[1] http://en.wikipedia.org/wiki/High-energy_physics

[2] http://en.wikipedia.org/wiki/Observational_astronomy

[3] Por ejemplo, http://en.wikipedia.org/wiki/List_of_largest_optical_reflecting_telescopes, http://en.wikipedia.org/wiki/X-ray_telescope

[4] http://en.wikipedia.org/wiki/Large_Hadron_Collider

[5] http://en.wikipedia.org/wiki/Higgs_boson

¿Es posible medir?

Cuando las circunstancias o los apóstoles de la seguridad lógica consiguen llamar la atención sobre la Seguridad en los Sistemas de Información, los directivos siempre terminan planteando si es posible "*medir*", de alguna forma, lo que se gana invirtiendo en seguridad informática. Solo es esperable la inversión y el reconocimiento de méritos a la Seguridad Lógica si se obtiene un resultado favorable en esa medida de las ganancias que van asociadas con ella.

Esencialmente, toda medida es un convenio por el cual se asignan números a objetos o eventos. Todas las medidas científicas tienen, básicamente, tres componentes: la magnitud, las dimensiones o unidades y su incertidumbre. En ciencia y tecnología las medidas se utilizan para hacer comparaciones entre observaciones distintas y así reducir (estadísticamente) la confusión y aprender algo con ello. Sin embargo, en el mundo empresarial, más que de medidas científicas, de lo que se habla es de KPIs.

Si queremos construir KPIs que realmente nos informen de lo seguro que es nuestro sistema, invirtamos continuamente dinero y esfuerzo en romperlos y así poder ser nosotros los primeros en enterarnos de que se pueden romper y abandonarlos tan pronto como sea posible para mitigar los efectos de su hundimiento.

Los *Key Performance Indicators*

Los *Key Performance Indicators*[6] son constructos que, periódicamente, se evalúan para "*conocer*" las capacidades de las organizaciones en función del comportamiento, lo más real y preciso posible, de sus unidades de negocio, de sus departamentos y, como no podía ser de otro modo, de sus empleados. Dado el uso que se hace de ellos, los KPIs deben ser comprensibles, tener (más o menos) sentido para el común de los mortales y deben ser mensurables.

En general, los indicadores de eficacia excluyen de su ecuación cualquier factor que sea incontrolable o dependa (directamente) de la subjetividad de las personas. Dada su naturaleza relativa, estos parámetros empresariales siempre se refieren a "*valores objetivo*" u "*objetivos estratégicos*", de modo que el valor de la medida está relacionado cuantitativamente con la consecución o no de esos objetivos. A fin de cuentas, los KPIs son métricas del éxito y del fracaso.

El KPI a menudo se elige asociado con el uso de distintas técnicas para descubrir cuál es el estado presente del negocio y de sus actividades principales y, en algunas ocasiones, estas medidas conducen a la identificación de mejoras potenciales, por lo que esos indicadores teleológicos[7] suelen estar relacionados con "*iniciativas de mejora de la productividad*".

Algunos ejemplos de KPIs relacionados con las tecnologías de la información bien podrían ser: la disponibilidad[8], el tiempo medio entre fallos[9], tiempo medio hasta reparación[10], la tasa de indisponibilidad no planificada, etc., pero ¿cuáles son los KPIs específicos de la seguridad lógica? **¿Cómo se puede medir el éxito de las medidas preventivas? ¿Cómo se puede establecer el beneficio de lo que no ocurre?**

En ciencia y tecnología las medidas se utilizan para hacer comparaciones entre observaciones distintas y así reducir (estadísticamente) la confusión y aprender algo con ello. Sin embargo, en el mundo empresarial, más que de medidas científicas, de lo que se habla es de KPIs.

El objetivo esencial de la seguridad lógica es mantener controlada la difusión de la información (confidencialidad), el acceso a la misma (autorización), poder verificar su entereza frente a errores fortuitos o ataques inteligentes (integridad), distinguir agentes involucrados (identidad), gestionar autorizaciones (potestades), establecer secuencias causales incontestables (firma digital), etc.

Medición y KPIs

Así pues, sería necesario contar con KPIs que permitan "*medir*" lo fuerte, robusto y resistente que es un sistema criptográfico para preservar, por ejemplo, la confidencialidad de una información (algoritmo criptográfico, gestión de claves, protocolos de actuación, mantenimiento, verificación, salvaguardia, etc.). Dado que en este ejemplo lo que se persigue es que nadie que desconozca la clave secreta pueda acceder a la información o pueda modificarla, su indicador no sería cuantitativo, sino cualitativo (ocurre o no ocurre) y, además, ese indicador no podría ser medido, ya que toda medida (científica) requiere determinar estadísticamente una magnitud y su incertidumbre asociada.

Los KPIs[11] en criptografía se parecen, en parte, a las pruebas de resistencia de materiales. Para saber cuánto resiste el pilar de hormigón de un viaducto se preparan varias muestras de hormi-

[6] http://en.wikipedia.org/wiki/Performance_indicator
[7] http://en.wikipedia.org/wiki/Teleology
[8] http://en.wikipedia.org/wiki/Availability
[9] http://en.wikipedia.org/wiki/Mean_time_between_failure
[10] http://en.wikipedia.org/wiki/Mean_time_to_repair
[11] http://en.wikipedia.org/wiki/Strength_of_materials

gón idénticas en todo a las que hay en la estructura que se quiere certificar. A esas muestras se las somete a presiones crecientes hasta que una tras otra revientan. Con varias pruebas en condiciones controladas (idénticas) se puede estimar cuál es la presión (media) a la que termina rompiendo ese hormigón en particular y lo grandes o pequeñas que son las desviaciones estadísticas respecto a esa valor medio experimental.

En criptografía no hay posibilidad de preparar varias muestras; con que hubiese un solo caso en el que alguien pueda romper un sistema criptográfico, dicho sistema debe ser abandonado de inmediato puesto que un ataque criptoanalítico solo puede mejorar con el paso del tiempo.

El caso de la criptografía

En criptografía hay dos grandes tipos de seguridades: **1)** la de que no se haya oído de nadie capaz de romper un sistema criptográfico (descubrir la clave) con eficiencia mayor que la de ir probando todas las claves (seguridad computacional), y **2)** la de que el sistema incluye claves que conducen a "*cifrados débiles*" (rompibles) pero estas son pocas, están dispersas y son imposibles de encontrar cuando las buscas; por lo que, en esos casos, "*es posible, pero muy poco probable darse de bruces con ellas*" (seguridad probabilística). El problema es que cuando una información deja de ser secreta, cuando se quiebra su confidencialidad, es imposible repararla.

Además del caso de la resistencia de materiales, otro ejemplo lo podríamos ver en las represas que interrumpen y controlan el flujo de algunos ríos. Cuando en cualquiera de ellas se produzca la más mínima fisura y el agua retenida se abra camino a través de ella, es cuestión de horas o minutos que la fisura se haga agujero. Este boquete, por el que el agua a velocidad desmedida, arrastrará violentamente todo el muro de contención dejando libre una cuenca montañosa entera llena de unas aguas [12] que lo arrastraran todo [13].

En los ejemplos anteriores, los fallos en los materiales o en la estabilidad de las represas pueden estar propiciados e incluso favorecidos, por el incumplimiento de ciertas obligaciones técnicas y profesionales a la hora de construirlas (aluminosis del hormigón [14]) pero, aún en ausencia de estos vicios, no es posible predecir cuándo se va a producir el desastre. Lo mismo ocurre con los fenómenos sísmicos y los terremotos. La geología y la teoría de las placas continentales apuntan a que algo gordo tiene que pasar en la Falla de San Andrés [15] de California, pero nadie sabe cuándo ocurrirá [16].

Los sistemas criptográficos son seguros hasta el día en que dejan de serlo, y cualquier indicio de debilidad debe ser tomado como el epílogo del mismo. Desde siempre, **la única posibilidad para establecer la seguridad de los sistemas criptográficos es intentar continuamente romperlos y abandonarlos tan pronto flojeen**.

KPIs que informen

Si queremos construir KPIs que realmente nos informen de lo seguro que es nuestro sistema, **invirtamos continuamente dinero y esfuerzo en romperlos y así poder ser nosotros los primeros en enterarnos de que se pueden romper** y abandonarlos tan pronto como sea posible para mitigar los efectos de su hundimiento. Si el contraespionaje alemán [17] hubiese estudiado mejor su máquina Enigma y hubiese, simplemente, empezado a sospechar de su resistencia [18], probablemente habría pasado a utilizar otras máquinas de cifrado en sus comunicaciones y la ventaja de los aliados se habría esfumado [19]; y quién sabe, quizás hubieran cosechado otro resultado en aquella sangrienta guerra.

Para evitar que sean los ciberdelincuentes, los *hacktivistas* de Anonymous o los *ciberwarriors* de quién sabe qué oscuras potencias o agencias los que se nos cuelen hasta la cocina en nuestros sistemas, **debemos disponer de equipos independientes e inmejorablemente preparados para atacarnos continuamente**. Esos equipos deberán contar con nuestro permiso y financiación a cambio de que seamos nosotros los que nos enteremos primero de por dónde se puede entrar y tener así la posibilidad de mitigar efectos y reparar fisuras. Si quieres proteger tu información, es sencillo: forma y contrata buenos criptoanalistas y hackers. ■

Debemos disponer de equipos independientes e inmejorablemente preparados para atacarnos continuamente. Esos equipos deberán contar con nuestro permiso y financiación a cambio de que seamos nosotros los que nos enteremos primero de por dónde se puede entrar y tener así la posibilidad de mitigar efectos y reparar fisuras.

[12] http://es.wikipedia.org/wiki/Rotura_de_presa

[13] http://en.wikipedia.org/wiki/Shimantan_Dam

[14] http://es.wikipedia.org/wiki/Aluminosis

[15] http://en.wikipedia.org/wiki/San_Andreas_Fault

[16] http://en.wikipedia.org/wiki/Earthquake_prediction

[17] R. A. Ratcliff: *"Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers"*. Cambridge University Press, 1st edition (October 6, 2008) ISBN-13: 978-0521736626

[18] http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

[19] http://en.wikipedia.org/wiki/Ultra

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es