



Actuando a la sombra del futuro

Una actividad tan habitual como es la transferencia de riesgos a través de seguros y otros tipos de acuerdos de mutuo socorro, no ha colonizado todavía el espacio que hoy representa Internet y el Ciberespacio. Es raro que ese establecimiento esté tardando tanto y quizás sea interesante indagar el porqué de esa ausencia. Es tiempo de que intentemos ver en qué consiste el problema y cuál puede ser la explicación de que las compañías de seguros no estén asegurando los procesos de Internet.

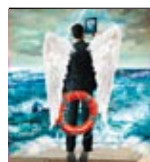
Cuenta Herodoto² que hubo un tal Polícrates³, tirano de la isla de Samos, que una vez en el poder, estableció vínculos de hospitalidad con Amasis⁴, rey de Egipto, al que enviaba presentes y de quien lo recibía.

El poderío de Polícrates creció rápidamente y su fama se extendió por Jonia y el resto de Grecia. Cada vez que se lanzaba a una guerra, fuera donde fuera, todas sus campañas se desarrollaban favorablemente. Con sus cien penteconeros y sus mil arqueros, saqueaba y pillaba de todo el mundo, sin hacer excepción con nadie, pues creía que "se queda mejor con un amigo devolviéndole lo que le ha arrebatado que sin quitarle nada".

alma y que, cuando lo hubiese encontrado, se deshiciera de ello de manera que nunca pudiera llegar a manos de otro hombre.

encontraron en su tripa el anillo de Polícrates. Nada más verlo, lo cogieron y llenos de alegría fueron a llevárselo explicándole de qué manera

Al cabo de poco tiempo Amasis supo que uno de los sátrapas del rey de Persia atacó Samos, apresó a Polícrates y lo mandó crucificar.



Si nos movemos al escenario de Internet también es necesario conocer íntimamente las cualidades, capacidades y caprichos de los sistemas de información que son los objetivos o el medio para realizar los ataques; es decir, de los eventos indeseables que cada día son más ciertos.

Leídas estas líneas y comprendiendo el acertado consejo de Amasis, Polícrates buscó entre los objetos más preciados, aquel por cuya pérdida mayor pesar le haría sentir, y dio con un sello engastado en oro y coronado con una esmeralda. Una vez decidido a deshacerse de

había sucedido. Sorprendido Polícrates redactó una carta contando lo sucedido y la envió a Egipto.

Cuando Amasis leyó la carta comprendió que era imposible librar a Polícrates de su destino y que no iba a tener un final feliz, pues tenía tanta suerte que hasta encon-

A la sombra de un beneficio futuro

La causalidad aristotélica⁵ nos hace creer que decisiones que tomamos ahora tienen efecto sobre el futuro, por lo que algunas de **nuestras decisiones presentes se toman bajo la sombra de un beneficio futuro**. Es esa sombra del futuro lo que movió a Amasis a olvidar a su amigo antes que tenerlo que llorar.

Más de dos mil años después, el futuro que le espera en Internet a cualquier sistema de información, a cualquier red de monitorización y control industrial que acumule algún tipo de éxito, poder o atractivo, es el de ser víctima de un ataque específico que podrá terminar con el negocio que sustenta. La envidia de los dioses, o mejor, de aquellos



Hay que recordar lo difícil que es, en general, la cuantificación de las pérdidas reputacionales¹, pero en el caso de Internet esa cuantificación probablemente es imposible.

El faraón Amasis no dejaba de prestar atención a la enorme suerte de Polícrates y envió a Samos una carta en la que le decía que esos grandes éxitos no le llenan de satisfacción, pues la divinidad es envidiosa y todavía no había oído hablar de nadie que, pese a triunfar en todo, a la postre no haya acabado desgraciadamente sus días. Como solución a ese negro destino, le propuso que eligiese algo que tuviera en máxima estima y cuya pérdida le dolería profundamente en el

aquella alhaja, embarcó en una nave y puso rumbo a alta mar. Al estar suficientemente lejos de la isla, se quitó el sello y lo arrojó al mar a la vista de todos. Después regresó a su palacio y dio rienda suelta a su tristeza.

A los cuatro o cinco días, un pescador cogió un enorme y magnífico pez del que pensó merecía ser un regalo para su señor. Lo llevó a palacio y allí lo entregó como un presente para el tirano. Al abrir las entrañas del pez, los servidores

traba las cosas que quería perder. Mandó un emisario a Samos e hizo saber que daba por cancelado su vínculo de hospitalidad para evitarse el disgusto personal que sentiría cuando le sobreviniera una terrible y enorme desgracia.

¹ Ver http://en.wikipedia.org/wiki/Reputational_risk

² Herodoto, Historias Libro III [3.39^a 3.43]

³ Polícrates (570 ac-522 ac.), hijo de Eaces y poderoso tirano de la isla de Samos entre el 540 ac. y el 522 ac.

⁴ Amosis II o Amasis (570 - 526 ac.) fue faraón de la dinastía XXVI de Egipto, último gran gobernante de Egipto antes de su conquista por Persia.

⁵ Ver http://en.wikipedia.org/wiki/Posterior_Analytics

que tengan poder real en Internet, no se va a limitar a hacer un uso civilizado, democrático y altruista de ella; sino que intentarán sacar el máximo beneficio de sus competidores o de las almas cándidas que puedan encontrar en el ciberespacio. El anunciado desastre de Polícrates es el mismo que debe esperar cualquier empresa "apetecible" en Internet.

En esta historia, es curioso el papel de Amasis que sabe retirarse a tiempo para que no le arrastre de algún modo el desastre de su, hasta entonces, amigo. Su estrategia es la que desearía para sí cualquier Agencia de Seguros que pudiese reconocer el riesgo de sus clientes y que, con el procedimiento del anillo, pudiese evaluar, **medir la inminencia del desastre.**

del impacto financiero del riesgo y la incertidumbre en una entidad o colectivo. Si la curiosidad lo propicia, un buen ejemplo divulgativo de esa disciplina lo podemos encontrar en la monografía



Si la mitad del éxito de los actuarios está en la calidad de las estadísticas (probabilidades) que utilizan, ¿cuáles son las estadísticas que van a utilizar para medir el riesgo de un ataque Avanzado, Persistente y Dirigido? Otra forma de hacer esa misma pregunta es si hay casos y datos suficientes para estimar correctamente las probabilidades de cada uno de esos insidiosos y peligrosos ataques.

"Fundamental Concepts of Actuarial Science" de Charles L. Trowbridge (1989).

Según ese autor, "*el utilitarismo⁶ y la aversión psicológica al riesgo es lo que da lugar a los sistemas de seguridad financiera como mecanismos para reducir las consecuencias financieras de eventos desfa-*

incierto (cuantía asegurada). Cuando la pérdida económica no puede evitarse, siempre puede compartirse. La idea básica es que se puede reunir el riesgo económico de todo un colectivo **de modo**

estocásticos que permiten evaluaciones de riesgo más complejas. Por si eso fuera poco, el surgimiento de lo que se ha dado en denominar "Big Data" va a suponer el análisis rutinario de inmensas

que pequeñas pérdidas de muchos puedan compensar grandes pérdidas de unos pocos. Así pues, "los seguros" son un sistema económico diseñado para transferir riesgo económico del individuo a un agregado o colectividad de individuos, o de un colectivo a otro.

cantidades de información de todo tipo.

En el campo general de los seguros, la calidad de esas estimaciones depende directamente de la capacidad de análisis, del conocimiento del negocio y de la comprensión precisa de la conducta humana que tenga el actuario. Sin embargo, si nos movemos al escenario de Internet, además de todo lo anterior, también es necesario conocer íntimamente las cualidades, capacidades y caprichos de los sistemas de información que son los objetivos o el medio para realizar los ataques; es decir, de los eventos indeseables que cada día son más ciertos. Aquí se podría reutilizar una narración que tuvo mucho éxito en la Edad Media europea y que es **la Parábola de las diez vírgenes⁸.** En Internet, lo que sin duda llegará no es el deseado novio, sino el ataque informático que nos deje fuera de juego.

En esencia, los Actuarios evalúan la **probabilidad de los eventos** que son capaces de imaginar y **cuantifican los resultados contingentes** con el fin de minimizar los impactos de las pérdidas financieras asociadas con eventos indeseables e inciertos.

La probabilidad

La cuantificación de los resultados contingentes quizás



Son demasiadas las preguntas que podemos hacer sobre la amenaza y muy pocos los casos bien conocidos, por lo que la confección de estadísticas es imposible. Por si fuera poco, no es un problema de tiempo. El tema requiere más análisis y mucha más dedicación, pero ahora ya no está claro que el clásico procedimiento de estimación de riesgos y costes derivados de esos riesgos, pueda funcionar en Internet.

La evaluación del impacto financiero del riesgo y la incertidumbre

En nuestros días, las estimaciones de Amasis hubiesen sido un ejemplo más de lo que se denomina "**Ciencia Actuarial**"; que es una disciplina que, armada de modelos estadísticos y matemáticos, persigue poder evaluar riesgos y con ello servir de criterio para los sectores asegurador y financiero. Por ello, los "actuarios" son aquellos profesionales encargados de la gestión y **evaluación**

vorables". Y en ese escenario "*los Actuarios son aquellos profesionales que tienen una comprensión profunda de los sistemas financieros de seguridad, sus razones de ser, su complejidad, sus matemáticas y su forma de trabajar*".

Efectivamente, esos procedimientos financieros crecen en respuesta al poco gusto de la mayoría de los usuarios a correr riesgos económicos. De hecho, muchos están dispuestos a asumir una pérdida menor pero cierta (la prima del seguro), en lugar de tener que lidiar, solo y por su cuenta, con una pérdida aún mayor pero

¿Se pueden asegurar las consecuencias de ataques intencionados?

La pregunta que nos podemos hacer ahora es si siempre se puede recurrir a esta solución financiera, si se puede asegurar cualquier cosa y, en particular, si **se pueden asegurar las consecuencias de ataques intencionados sufridos en el ciberespacio.**

Históricamente, la ciencia actuarial ha utilizado modelos deterministas para la construcción de Tablas de Vida⁷ y el cálculo de primas. La ciencia actuarial ha cambiado mucho con el desarrollo de los ordenadores, lo que ha abierto la puerta a **modelos actuariales**

⁶ Ver <http://en.wikipedia.org/wiki/Utilitarianism>

⁷ Ver http://en.wikipedia.org/wiki/Life_table

⁸ Mateo 25:1-13 Parábola de las diez vírgenes

no se vea muy cambiada por pasar a escenarios en Internet, siempre y cuando sigan afectando a bienes externos al propio medio cibernético. Hay que recordar lo difícil que es,

De acuerdo con esta ley, el valor de la media de los resultados obtenidos para un número grande de pruebas estará cada vez más cerca del valor esperado, acercán-

cosas tan básicas como saber: (1) por dónde van a entrar (*exploit*), (2) de qué forma se va a cargar en el equipo infectado (*packers* polimórficos), (3) qué cabeza de puente van

estimar riesgos en el modo clásico que los actuarios lo han hecho en los últimos cien años.

El tema sin duda requiere más análisis y mucha más dedicación, pero ahora ya no está claro que el clásico procedimiento de estimación de riesgos y costes derivados de esos riesgos, pueda funcionar en Internet. Quizás se pueda tratar "estadísticamente" en fraude financiero de tarjetas a través de Internet (de hecho son muchos los que lo hacen) porque en ese escenario sí son millones los casos, los eventos de fraude detectados, auditados y, por lo tanto, analizables estadísticamente.

Sin embargo, el espionaje, la extorsión y el secuestro "adaptado y dirigido" son creaciones prácticamente únicas, son obras de autor, operas primas de artista que se escapan a la fría herramienta estadística de las compañías de seguros con las que transfieren el riesgo entre otros, pero de tal modo



Quizás se pueda tratar "estadísticamente" en fraude financiero de tarjetas a través de Internet (de hecho son muchos los que lo hacen) porque en ese escenario sí son millones los casos, los eventos de fraude detectados, auditados y, por lo tanto, analizables estadísticamente.

en general, la cuantificación de las **pérdidas reputacionales**⁹, pero en el caso de Internet esa cuantificación probablemente es imposible.

Lo que si cambia radicalmente en el caso de los ciberataques es poder basarse en el uso de probabilidades. **¿Cuál es la probabilidad de un APT?**¹⁰, entendiendo por "probabilidad" una **medida matemática**¹¹ de la posibilidad de que un determinado evento ocurra.

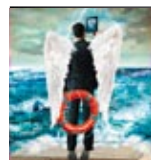
La probabilidad tiene su formalización axiomática en la **Teoría de la Probabilidad** que se encarga del análisis de los fenómenos aleatorios y que está en la base de la **Estadística**, las finanzas y los juegos de azar, la ciencia básica, la inteligencia artificial y el aprendizaje de las máquinas para **diseñar inferencias sobre la frecuencia esperada de los eventos**.

La Teoría de la Probabilidad es esencial en el **análisis cuantitativo de grandes conjuntos de datos**. Dos grandes ejemplos de ello son el **Teorema del Límite Central**¹² y la **Ley de los Grandes Números**¹³. Esta última es un teorema que describe el resultado que se obtiene al realizar muchas veces el mismo experimento.

dose más y más según se vayan haciendo más pruebas. **Gerolamo Cardano** (1501–1576) fue el primero que afirmó, sin probarlo, que la precisión de las estadísticas experimentales tienden a mejorar con el número de pruebas realizadas.

Si la mitad del éxito de los actuarios está en la calidad de las estadísticas (probabilidades) que utilizan, ¿cuáles son las estadísticas que van a utilizar para medir el riesgo de un ataque Avanzado, Persistente y Dirigido? Otra forma de ha-

a establecer (*rootkit*), (4) qué mecanismo de control van a seguir (*C&C botnet*), (5) qué mecanismo de comunicación van a utilizar (mensajes DNS, POST en http, mensajes en Twitter, entregas en Pastebin, charlas IRC, etc.), (6) qué técnicas de descubrimiento de lo que buscan van a utilizar, (7) cómo van a recopilar los datos que buscan, (8) cómo van realizar sus acciones de espionaje, (9) cómo van a exfiltrar el botín que consigan, (10) qué medidas anti-forense van a utilizar, entre otras cosas.



El espionaje, la extorsión y el secuestro "adaptado y dirigido" son creaciones prácticamente únicas, son obras de autor, operas primas de artista que se escapan a la fría herramienta estadística de las compañías de seguros con las que transfieren el riesgo entre otros, pero de tal modo que nunca les afecte a ellas y a su beneficios.

cer esa misma pregunta es si hay casos y datos suficientes para estimar correctamente las probabilidades de cada uno de esos insidiosos y peligrosos ataques.

Hace poco que saltaron esas tan manoseadas siglas APT a la palestra, por lo que podría aceptarse que no haya suficientes casos para tener estadísticas útiles y fiables, sobre

Son demasiadas las preguntas que podemos hacer sobre la amenaza y muy pocos los casos bien conocidos, por lo que la confección de estadísticas es imposible. Por si fuera poco, no es un problema de tiempo. El *malware* y las ciberarmas tienen una característica esencial y es la de **no servir para muchas campañas**, sobre todo si el arma ha sido diseñada con especificidad para su objetivo. Con ataques tan adaptados es imposible que en algún momento pueda haber muestras suficientes para poder establecer probabilidades y con ello

que nunca les afecte a ellas y a su beneficios. El pastel de Internet precisa de nuevas herramientas y enfoques para que pueda ser servido en la mesa de las compañías aseguradoras. ■

JORGE DÁVILA
Consultor independiente
Director
Laboratorio de Criptografía
**LSIS – Facultad
de Informática – UPM**
jdavila@fi.upm.es

⁹ Ver http://en.wikipedia.org/wiki/Reputational_risk

¹⁰ Ver http://en.wikipedia.org/wiki/Advanced_persistent_threat

¹¹ Ver [http://en.wikipedia.org/wiki/Measure_\(mathematics\)](http://en.wikipedia.org/wiki/Measure_(mathematics))

¹² Sobre la suma de n variables aleatorias independientes y de varianzas no nula pero finita. Ver http://en.wikipedia.org/wiki/Central_limit_theorem

¹³ Sobre el comportamiento del promedio de una sucesión de variables aleatorias según aumenta el número de ensayos. Ver http://en.wikipedia.org/wiki/Law_of_large_numbers