novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*), representa a España en **IFIP** (*International Federation for Information Processing*) y es miembro de **CLEI** (*Centro Latinoamericano de Estudios de Informática*) y de **CECUA** (*Confederation of European Computer User Associations*). Asimismo tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*) y colabora con diversas asociaciones informáticas españolas.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Gutierre de Cetina 24, 28017 Madrid •Tlfn.914029391 <novatica@ati.es>
Administración y Redacción ATI Cataluña
Calle Ávila 50, 3a planta, local 9, 08005 Barcelona
Tlfn.934125235 <secregen@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Gutierre de Cetina 24, 28017 Madrid
Tlnf.914029391 <novatica@ati.es>
Imprenta: Impresión Offset Derra S.L., Llull 41, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: "El guardián" - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 238, noviembre 2016 - febrero 2017, año XLII

Monografía del próximo número: "Salud y tecnología"

El ciberpuzle. Cómo el sentido común puede resolverlo

John McCarthy
Director General de Oxford Systems (Reino Unido)

<john.mccarthy@oxfordsystems.co.uk>

Traducción: Miguel García-Menéndez (Vicepresidente de ATI, editor invitado de la monografía).

Resumen: *A lo largo de este artículo, el autor intenta poner de relieve los problemas a los que, hoy, se enfrenta quien trata de entender las incógnitas que se ciernen en torno a la seguridad digital. Sugiere que los puntos de vista que se han tomado tradicionalmente al hablar de seguridad no siempre resultan de ayuda cuando se trata de este nuevo ámbito, el digital. Como consecuencia, opta por mirar más allá de la tecnología, examinar los problemas desde una perspectiva humana y ofrecerle, como lector, una batería de soluciones sencillas que le permitan mitigar muchas de las ciberamenazas actuales. Finalmente, defiende que no se trata de un problema que uno pueda abordar en solitario, sino que requiere de un nuevo nivel de interacción entre organizaciones, que permita atajar las amenazas de hoy y de mañana.*

Palabras clave: *cíber, ciberhigiene, ciudad inteligente, cultura, Internet de las Cosas, IoT, SCADA, seguridad digital,* smart city.

Autor

John McCarthy es una autoridad en estrategia, desarrollo y puesta en marcha de programas de seguridad digital. Obtuvo su doctorado en Ciberseguridad y Desarrollo de Negocios Electrónicos y es un autor reconocido internacionalmente. Entre sus escritos se cuenta una serie de informes académicos que recogen todos los aspectos de la seguridad digital en el mundo moderno. Asimismo, comparte regularmente sus reflexiones, en forma de pequeñas píldoras, que publica como entradas en la bitácora electrónica de Oxford Systems <http://www.oxfordsystems.eu/index.php/blogs>. Es un destacado instructor y experto en buenas prácticas y concienciación en materia de ingeniería social, disciplina sobre la que versará su próximo libro. McCarthy participa frecuentemente como experto invitado en grupos de trabajo y como ponente en reputadas conferencias internacionales de seguridad digital. Colabora en un notable número de destacados comités estadounidenses que prestan asesoramiento y orientación sobre políticas en materia de seguridad digital a la Administración de los EE.UU. Forma parte del grupo de expertos del Comité Estadounidense de Investigación para el Transporte, que está trabajando sobre las mejores prácticas de seguridad digital para los aeropuertos ubicados a lo largo y ancho de los EE.UU. Es un activo miembro del Comité de Seguridad en la Aviación de ACI Europe, la vertiente europea del Consejo Internacional de Aeropuertos; de la Sociedad Informática Británica (BCS, por sus siglas en inglés) y de su foro de liderazgo en Tecnologías de la Información, ELITE; del Comité Internacional de Guerra de la Información y Seguridad; y de la organización no gubernamental londinense "The Worshipful Company of Information Technologists". Además, John ostenta el honor de ser un "Freeman" (Hombre Libre) de la Ciudad de Londres. En la actualidad, el Dr. McCarthy es el Director General de Oxford Systems.

1. El Salvaje Oeste

Se dice a menudo que Internet es una nueva frontera, preparada para ser descubierta y explorada. A veces se aprecia un paralelismo entre el ciberespacio y el Salvaje Oeste. En cierto modo, dicho paralelismo es cierto. Tanto el Salvaje Oeste, como el ciberespacio son dos territorios sin ley, en los que los delincuentes pueden actuar y actúan con impunidad. Muchos colectivos marginados presintieron la libertad del Salvaje Oeste y emigraron a los EE.UU. donde pudieron actuar y comportarse a su antojo. Esos mismos grupos, hoy, pueden estar utilizando Internet como plataforma para sus intereses; unos intereses que podrían no ser bien vistos en cualquier otro lugar.

Tanto Internet como el Salvaje Oeste son dominios carentes, o que carecieron, de censura. Para algunos este espíritu pionero es lo que resulta atractivo; sin embargo, para otros es motivo de preocupación. Una diferencia fundamental es que el Salvaje Oeste era un lugar concreto. Uno viajaba a él o lo evitaba, según su voluntad. Internet no cuenta con una ubicación física específica y, aunque también se la puede probar o evitar, en las economías desarrolladas resulta ubicua. Toca cada aspecto de la vida de la gente [2]. Incluso aunque alguien no la *use*, todo el mundo a su alrededor lo hará, así que no hay escapatoria.

Dicha diferencia no puede obviarse. En el pasado uno podía sentarse en su civilizado hogar y hablar sobre los peligros y depravaciones del Salvaje Oeste, plenamente consciente de que a menos que lo visitase, permanecía seguro. No puede decirse lo mismo de Internet. Sus peligros rodean a todo el mundo, a sus hijos y a sus negocios. A la gente le gusta pensar que Internet es *segura*. Puede ser muy segura y un completo descontrol al mismo tiempo. Es necesario entender esta dicotomía, algo que los gobiernos también se esfuerzan por comprender.

En el Salvaje Oeste, en última instancia, el problema se resolvió ligando la ubicación física y la seguridad. Se llevaron alguaciles y eso permitió tener una idea, más o menos clara, de lo que estaba seguro y protegido. No se puede aplicar esta solución a Internet, dado que no tiene ubicación. Pueden hacerse algunas cosas, por ejemplo, uno puede mantener su propia casa en orden; pero se trata de una solución muy limitada. Se ha creado un mundo donde todo está conectado a todo lo demás: *Internet de las Cosas* (IoT, por sus siglas en inglés) y *Ciudades Inteligentes* (del inglés *smart cities*) son dos expresiones que están de moda, aunque lo cierto es que los conceptos subyacentes son, ya, una realidad. Un débil enlace interconectado se convertirá en el enlace débil de todo el mundo. Mucha gente, simplemente, no está preparada para asumir que la seguridad digital va más allá de las fronteras internacionales o de las legislaciones. Es natural que cada uno reaccione en función de dónde está. Tristemente, esto resulta de poca ayuda en el dominio de *lo cíber*.

2. Proteger la propia casa

Si se es **víctima de un ciberdelito, las opciones de** que atrapen a los delincuentes son muy escasas. Probablemente habrán actuado desde otro país y, por tanto, el sistema legal de protección tendrá que vérselas con las dificultades derivadas de las diferentes jurisdicciones y del propio ciberdelito. Internet no respeta los estados soberanos. Por ejemplo, si enviamos un mensaje de correo electrónico, éste podría recorrer todo el mundo antes de alcanzar su destino; un destino, tal vez, muy cercano. Los protocolos que se utilizan en Internet están diseñados para eso.

A medida que la seguridad digital se va introduciendo en el ideario colectivo, con

> “ Existe la creencia general de que todos los sistemas pueden ser atacados y de que no hay nada a salvo de los atacantes ”

frecuencia, también se contamina por historias glamurosas de atacantes despiadados e inteligentes que han explotado sistemas por valor de millones de dólares. Existe la creencia general de que todos los sistemas pueden ser atacados y de que no hay nada a salvo de los atacantes. En el mundo de lo absoluto, en el que uno tiene en cuenta cada posibilidad, nada está libre de ser atacado. Sin embargo, si aplicase esta forma de pensar a otras áreas de su vida cotidiana, vería que el pensamiento absoluto no siempre ayuda. Consideremos el ejemplo de la puerta de entrada de una casa. Contestemos a la siguiente pregunta, “*¿puede derribarse esa puerta y que la casa sea allanada?*”. La respuesta es un evidente “*sí*”. En las casas se colocan puertas que se consideran suficientemente seguras para el papel que se les encomienda. De ese modo, lo que se hace es adoptar un enfoque de análisis del riesgo para la seguridad del propio domicilio.

Una lógica pragmática como ésta constituye la base sobre la que están construidos muchos sistemas de seguridad digital. Sin embargo, el gran público piensa en términos absolutos cuando trata con los problemas de seguridad digital. Suelen hacerme muchas preguntas. Entre las más habituales está “*¿quién debería responsabilizarse por la seguridad digital de la organización?*”. Una pregunta perfectamente razonable y sensible.

La respuesta fácil no pasará de aquí y es ésta: “*El consejo de administración. Es un asunto que ha de tratarse a nivel de consejo*”. Una gran verdad y, en mi opinión, vital para una evaluación, despliegue y gestión exitosas de la seguridad digital. Las organizaciones necesitan colocar la seguridad digital en sus registros de riesgos y adoptar un marco regulatorio de referencia para administrarla.

Una vez que el consejo de administración haya *comprado* la idea, ¿bastará, simplemente, con entregar la seguridad digital al departamento de Informática? Bien, si eso es todo lo que se va a hacer, será más que factible que surjan problemas. El Departamento de Informática tiene un importante papel que jugar; pero, ¿qué hay del director de las instalaciones? A menudo, se trata de una figura que está a cargo de un montón de sistemas de control, conocidos como SCADA[1], que suelen ser vulnerables a ciberataques. Con certeza, hoy la seguridad digital también forma parte de las atribuciones de este otro perfil.

En muchas organizaciones la gestión de las instalaciones y el Departamento de Informática son entidades distintas y separadas. Unir ambos silos es uno de los desafíos existentes a la hora de desplegar una seguridad digital eficaz. Cómo se logre variará de una organización a otra; pero, en todo caso, requerirá el apoyo del Consejo de Administración.

3. Manipular a la persona

Es un dato conocido que más del 80% de los ciberataques están relacionados con algún tipo de error u omisión por parte de alguna persona [1].

Hagámonos esta pregunta: “*¿Dispone mi departamento de Informática de las destrezas y de la capacidad necesaria para formar a todos los empleados en cómo mitigar los ataques de ingeniería social?*”.

Todo el mundo ha visto en televisión programas sobre timadores y cómo roban dinero a víctimas inocentes. Sin embargo, si hablamos con algún artista del timo (y yo he conocido a unos pocos), siempre dirán que es la misma víctima quien termina siendo presa de su propia codicia. Eso puede ser verdad en ciertos casos en los que trucos así, pensados para vulnerar la confianza de la gente, muestran su eficacia; pero no en la vasta mayoría. En la mayor parte de las ocasiones estos embaucadores se aprovechan del hecho de que uno pueda estar ocupado, distraído o cansado; momento que eligen para actuar.

Esto hace que cualquiera sea susceptible de caer en un engaño de ingeniería social. A la fría luz del día todo el mundo es capaz de reconocer los trucos que emplean los timadores; pero ¿qué hay de un viernes por la tarde, cuando uno ya lleva todo el peso de la semana sobre sus hombros?

Si tenemos prisa tendemos a no concentrarnos tan bien y podemos resultar más vulnerables ante trucos inesperados. Por otro lado, si estás leyendo esto y tienes hijos, seguro que sabes todo lo que hay que saber sobre expertos ingenieros sociales. En resumen, cualquiera puede resultar engañado o persuadido.

Todo el mundo puede estar alerta cuando se le dice que alguien va a engañarlo. Pero, por desgracia, estas cosas no se avisan.

La respuesta a esto parece estar en la creación de una cultura de la seguridad digital que promueva una buena *ciberhigiene*. En ese supuesto, ¿no debería estar incluyéndose una formación básica en seguridad digital en el paquete de bienvenida para cada nuevo empleado? De ese modo, ahora, la seguridad digital amplía su alcance y cae bajo la potestad de RR.HH.

Hablar de Seguridad Digital es similar a hacerlo de Seguridad y Salud Laboral. Es una responsabilidad de todos, aunque algunas áreas juegan un papel y tienen unas obligaciones más complejas que el resto, como el Departamento de Informática. Otro ejemplo es el Departamento Contable, que requiere formación especializada en ingeniería social y un alto nivel de ciberhigiene para mantenerse verdaderamente vigilante. De hecho, todo empleado necesita estar al corriente de la seguridad digital y exhibir una buena ciberhigiene. El que esto comience a ser así, supone que se están empezando a dar pasos hacia una mayor protección de la organización frente a ciberataques. Si se adoptan buenas prácticas de seguridad digital, mediante la formación y la protección de los sistemas, se tendrá la oportunidad de promover esa buena seguridad digital como un activo de la organización. No cabe duda de que la seguridad digital comienza en lo más alto, pero es parte de las obligaciones de cada uno garantizar una buena seguridad. Para decirlo con claridad hay que insistir en que *la responsabilidad es de todos*.

En la era digital el problema de la ingeniería social tiene consecuencias mucho más graves. Ahora uno puede convertirse en una puerta de entrada hacia sistemas informáticos que los ingenieros sociales pueden emplear para desplegar software nocivo, robar información o destruir datos. ¿Por qué harían algo así?

Bien, la ingeniería social es un *oficio* que se mantiene por sí mismo y que ha estado ahí durante siglos; sin embargo, es ahora cuando está siendo usado como un vector de ataque para entrar en los sistemas más seguros. Esto ha provocado que muchos ha-

> “ Hablar de Seguridad Digital es similar a hacerlo de Seguridad y Salud Laboral ”

yan adoptado, junto a otras habituales artes del engaño, técnicas de ingeniería social.

Los delincuentes han sabido reconocer rápidamente que los sistemas informáticos, a pesar de estar protegidos mediante caros y sofisticados sistemas de cortafuegos y de detección de intrusiones, resultan muy fáciles de acceder a través de los humanos que los operan.

4. Crear una cultura de la seguridad digital y promover la ciberhigiene

Las respuestas no están en los sistemas informáticos, sino en la formación del personal para que sea consciente de la existencia de los ingenieros sociales y de los ataques que llevan a cabo. Un entrenamiento de carácter informativo, junto a la creación de una cultura de la seguridad digital y al desarrollo de unas buenas prácticas de ciberhigiene pueden hacer muchísimo en favor de la mitigación de este tipo de amenazas. Una buena cultura y una buena higiene son importantes, dado que refuerzan la formación impartida para mitigar las técnicas de ingeniería social.

Una sencilla ciberhigiene podría evitar muchos de los actuales ataques y problemas. No obstante, la comprensión de cómo se opera en este nuevo entorno es, aún, muy precaria para la mayoría. En otros ámbitos de la vida cotidiana se practica una buena higiene. La gente se lava las manos cuando sale del baño y se cubre cuando estornuda. Es necesario desarrollar prácticas de ciberhigiene similares, dentro y fuera de los lugares de trabajo. Comencemos por ellas. Impliquemos a toda la empresa, comenzando por lo más alto, y hagamos que quienes estén al frente den ejemplo. Se requieren mensajes sencillos sobre buenas prácticas de seguridad digital que todo el mundo, en cualquier nivel de la organización, pueda entender y adoptar.

Una vez se cuente con una buena cultura, todos los departamentos de la compañía entenderán las necesidades de los demás en materia de seguridad digital. Muchos de los obstáculos que se observan hoy en relación con acercar a las partes para resolver problemas de seguridad digital serán más fáciles de superar. Crear una meta común, utilizando un lenguaje familiar, será un gran avance a la hora de ayudar a promover una saludable cultura de la seguridad digital y, por tanto, a la hora de abordar muchos de los problemas que se padecen en la actualidad.

5. El problema en perspectiva

La seguridad digital toca todos los aspectos de la vida de una empresa, de forma que no cae fácilmente en un silo específico. Esto es así debido a que en los últimos años se ha experimentado un nuevo nivel de interconectividad entre dispositivos y sistemas; y, por tanto, para entenderlo completamente y para comprender su impacto sobre la seguridad digital se necesita examinar el problema desde más allá de las fronteras tradiciones de la lógica departamental.

Esto es desafiante para cualquiera, dado que todos están dispuestos a hacer lo necesario; pero, a menudo, nadie comprende plenamente el papel que le toca jugar. La cuestión pendiente, por tanto, sigue siendo ¿cómo crear una meta y alcanzar un resultado común para todos los afectados? Los implicados técnicos y del departamento de Informática querrán aplicar soluciones tecnológicas al problema de la seguridad digital y, en cierta medida, estarán acertados al pretenderlo. Los directivos pueden estar valorando una estrategia y una solución contraria al riesgo, mientras que la Administración querrá asegurarse de que se está haciendo todo lo necesario para proteger las infraestructuras críticas nacionales.

Entonces, ¿cuál es la respuesta? Recuerde este sencillo hecho: todos los negocios interactúan. En el ecosistema de los sistemas informáticos empresariales, estos están entrelazados a muchos niveles. Por tanto, centrarse en una gran empresa únicamente, es como poner una puerta acorazada a la entrada de su domicilio, mientras deja una ventana abierta en la parte de atrás. Cualquier solución de seguridad digital necesita abarcar cualquier tipo de empresa, grande y pequeña, para tener alguna opción real de triunfar. Se trata de una tarea desafiante y requiere un cambio de paso en las prácticas operativas de aquellas empresas que tienen diferentes propietarios, pero que tendrán que trabajar en equipo. Esto no se producirá de forma fácil, ni natural. Necesitará identificarse un objetivo común y especificarse un lenguaje que sea global en su alcance y comprensión. Todo el mundo debería situarse en la misma página. Es necesario crear una cultura de la seguridad digital donde todos interioricen la ciberhigiene y las buenas prácticas como parte de su forma natural de actuar.

Una reflexión final: si alguien cree que no es una víctima potencial de la ingeniería social, que sus puntos de vista y sus ideas no pueden ser manipulados, entonces deberá responder a esta cuestión, ¿cuándo fue la última vez que compraste, o quisiste comprar algo pensando sólo en la marca?[2]

Referencias

[1] CeBIT Australia. “The human factor in cyber security”. *17 de enero de 2016*. <http://blog.cebit.com.au/the-human-factor-in-cyber-security>.

[2] Instituto de Tendencias en Tecnología e Innovación (iTTi). El Manifiesto iTTi sobre el Gobierno Corporativo de las Tecnologías de la Información”. *1 de septiembre de 2014* http://es.slideshare.net/iTTi_news/el-manifiesto-itti>.

[3] John McCarthy. A word about cyber security (with Dr. John McCarthy)”. *Bitácora electrónica de Oxford Systems*. <http://www.oxfordsystems.eu/index.php/blogs>. Último acceso: 13 de febrero de 2017.

Notas

[1] Nombre genérico empleado, habitualmente, en referencia a los sistemas de automatización y control industrial (IACS, por sus siglas en inglés). Se trata de los sistemas de información que soportan las operaciones en plantas de producción (fábricas, centrales energéticas, etc.). Recientemente, este tipo de sistemas han adoptado la denominación “Tecnologías de Operación”, TO, por analogía a las “Tecnologías de Información”, TI, propias de entornos corporativos. Estrictamente hablando, los sistemas SCADA (*Supervisory Control And Data Acquisition* / Supervisión, Control y Adquisición de Datos) son un subgrupo dentro de los IACS o Tecnologías de Operación.

[2] Nota del editor: Si el lector está interesado en conocer más en profundidad los puntos de vista del autor, le recomendamos que consulte periódicamente el blog de su empresa, Oxford Systems [3].