DOCUMENTO DE REFLEXIONES DEL GRUPO DE TRABAJO "SEGURIDAD, ECONFIANZA Y FRAUDE EN INTERNET" DEL FORO DE LA GOBERNANZA DE INTERNET EN ESPAÑA

Nuevas tendencias de ataques y ciberfraudes

El fraude electrónico es cada vez más complejo desde el punto de vista técnico, se lleva a cabo de manera más personalizada a las particularidades del destinatario, y se está profesionalizando en su ejecución.

La diversificación y sofisticación es la tónica general. Cada vez tiene mayor relevancia el fraude basado en código malicioso o malware y la utilización de ingeniería social más específica para el destinatario. Tanto la BRIGADA DE INVESTIGACIÓN TECNOLÓGICA (BIT) como INTECO comparten la opinión, basada en su experiencia y sus estadísticas, que en el fraude online sigue funcionando la ingeniería social, pero también ataques con troyanos u otro tipo de malware, campañas coincidiendo con declaración del IRPF, eventos deportivos, noticias de actualidad, etc.

Así pues, se trata de ataques más complejos técnicamente, personalizados y organizados, y por todo ello, más difíciles de prevenir, identificar y combatir.

Además, la BIT indica que se están detectando ataques de ciberactivismo contra organismos públicos y partidos políticos.

Tanto INTECO y la BIT, como TELEFÓNICA y S21SEC comparten que está aumentado la variedad de dispositivos afectados: están siendo atacados los teléfonos y otros dispositivos móviles (*smartphones, tablets*, etc). En palabras de S21SEC, sin duda alguna el fraude online evoluciona en consonancia a la tecnología y plataforma más extendida, y en estos momentos es la tecnología móvil, principalmente teléfonos móviles y tablets la que está en el punto de mira de los ciberdelincuentes, ya que hoy día una mayoría de usuarios dispone de un terminal móvil inteligente, con capacidad de conectarse a la banca electrónica, gestionar correo o navegar por la web.

Enriqueciendo estas reflexiones y aportando nuevos datos, TELEFÓNICA indica que considerando la evolución de los servicios hacia entornos integrados fijo-móvil y la validación de los clientes, nos encontramos con:

- Robo de SMS de validación de transacciones bancarias a través de malware instalado en el terminal móvil.

- Identificación de la posición de terminales (seguimiento de personas) a través de aplicaciones que se basan en la información del GPS del terminal, transmitiendo hacia los delincuentes la posición física del móvil y, por tanto, de su titular.

- Captación de datos del cliente a través de aplicaciones simples o falsos juegos que en realidad son troyanos.

- Utilización de dispositivos móviles como partes de *botnets*: estas redes zombies, además de ordenadores, están migrando hacia dispositivos móviles, lo que permite hacer un balanceo de carga en los ataques de denegación de servicio a través de Internet, entre los equipos fijos y los móviles.

- Engaño a través de redes inalámbricas: los usuarios que utilizan wifi en sitios públicos se arriesgan a acceder a puntos de acceso comprometidos o activados con el objetivo de utilizar técnicas "*man in the middle*" para el robo de credenciales.

- Marcación a números de tarificación especial (906, 806) de voz o vía SMS/MMS realizado por malware para aumentar el ingreso de esos números.

- Deshabilitar el terminal móvil a través del uso de alguna vulnerabilidad del modelo.

- Robo de agendas con teléfonos y direcciones a través de malware o troyanos, con el fin de disponer de datos válidos de personas.

Como medios de distribución, S21SEC señala que es destacable el incremento del uso de las redes sociales para la propagación de malware unido a las conocidas técnicas de Black Hat SEO, que aprovechan la aparición de noticias impactantes (ej: el terremoto de Japón, la muerte de Bin Laden) para redirigir miles de usuarios a *"exploit kits"* preparados para infectar sus dispositivos. Los exploits además están evolucionando hacia tecnologías multiplataforma (java, pdf, swf), que prácticamente se encuentran en cualquier dispositivo, independientemente del hardware o el sistema operativo que usen.

La importancia de la detección temprana. La detección proactiva y la notificación por parte de las víctimas

La detención temprana de los intentos de fraude es crucial ya que permite actuar preventivamente a muchos organismos y actuar en ocasiones en el foco del ataque, sí como alertar a las potenciales víctimas y evitar perjuicios económicos posteriores.

Tanto la industria como la propia administración se nutre de información con origen en sensores que detectan la actividad maliciosa en la Red, a través de 3 canales: i) la propia víctima o usuario que detecta o sufre el incidente y que lo comunica al experto mediante los diversos canales; ii) la Administración, que en el caso de INTECO cuenta con una red de sensores de seguridad y un panel de usuarios y empresas en los que detecta incidentes de seguridad; iii) y la industria, que necesita de esta actualización constante de información para mejorar su tecnología y servicios hacia ciudadanos, empresas y administraciones.

Precisamente TELEFÓNICA pone de manifiesto la importancia de la detección proactiva por parte de la industria, por la vía de acciones de red y del software en los terminales. Las acciones desarrolladas en la red se basan en el análisis de tráfico sospechoso, a través de tanto sistemas de detección de virus en aplicaciones descargadas o tráfico

MMS, como de sistemas de detección de comportamiento anómalo de tráfico, esto es, detección de volúmenes de tráfico de SMS que un cliente no puede generar normalmente por sí mismo, detección de generación de tráfico especial para generar denegaciones de servicio contra un destino en concreto y otras acciones destinadas a identificar anomalías.

Este enfoque proactivo es una de las aproximaciones que puede resultar más interesantes, según S21SEC, desde el punto de vista de la inversión o ROSI (Return Of Security Investment) para proteger a las organizaciones de nuevas amenazas y riesgos de seguridad. Una visión proactiva de las nuevas amenazas permite, en parte, anticiparse o detectar con cierta agilidad nuevos riesgos y amenazas para la organización. Esta visión permitirá desplegar sistemas de seguridad acordes a las nuevas amenazas, además de ser una fuente de valiosa información para ajustar los sistemas reactivos existentes.

Para INTECO, la colaboración de los usuarios a la hora de evidenciar un intento de fraude es primordial para poder interceptarlos a tiempo y poder localizar lugares desde donde se publican páginas, se emiten mensajes fraudulentos o donde se reciben los datos capturados.

De cara a facilitar esta colaboración, la Oficina Seguridad del Internauta (OSI) pone a disposición del usuario el formulario de alta de incidentes, desde donde se puede indicar las entidades afectadas y toda la información disponible sobre el caso de fraude, y el teléfono de asistencia 901.111.121. En caso de haber sido víctima de un fraude, es conveniente poner inmediatamente la denuncia correspondiente, para lo que el usuario puede ponerse en contacto con la Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, con el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil o con las unidades especializadas de las Policías Autonómicas.

CIBERVOLUNTARIOS considera que conseguir una detección temprana pasa por el empoderamiento ciudadano, es decir, por el aumento de las capacidades, oportunidades y participación de las personas a través de todo tipo de herramientas, aplicaciones y servicios tecnológicos.

Según esta asociación es vital que cada uno de los ciudadanos sienta parte de la responsabilidad de lo que les sucede y formen parte activa en la prevención, detección y denuncia, si se llega a dar el caso. Que no se vean como meros receptores de todo tipo de aplicaciones proveniente de administraciones y empresas que les pueden y les deben de salvar. La detección temprana debe apoyarse en esa responsabilidad compartida, en un cambio de estrategia en el que desde el primer momento se trabaje con el ciudadano en la formación de su corresponsabilidad para garantizar su seguridad, basada en las correspondientes acciones de empoderamiento y participación tecnológica.

¿La delincuencia organizada se está profesionalizando y especializando en una materia como el fraude online o se dedican a todo?

La delincuencia organizada encuentra muy atractiva la Red para llevar a cabo sus actividades fraudulentas, ya que se trata de un entorno poco regulado, con escaso riesgo (o, en todo caso, mucho menor que en otras actividades delictivas como, por ejemplo, el tráfico de drogas) y donde pueden llegar a conseguir sustanciales sumas económicas.

Según la BIT de la Policía Nacional actualmente los grupos más activos son de origen ruso, latinoamericano (especialmente brasileños) y, últimamente, chino.

Por un lado, los grupos, generalmente pequeños, dedicados a los timos tradicionales, encuentran en Internet una oportunidad para seguir delinquiendo (cartas nigerianas, nazareno, falsas loterías, etc).

Por otro lado, surgen organizaciones más estructuradas, que se dedican al fraude online con una perfecta operativa: se produce un fenómeno que se ha venido a llamar *"crime as a service".* Los ciberdelincuentes disponen de estructuras organizativas complejas, que incluyen tareas de reclutamiento de "muleros" para el blanqueo del capital y un volumen creciente de recursos para la infraestructura técnica de los fraudes electrónicos. Unos tienen la infraestructura para recoger el dinero a través de las "mulas" y compran desarrollos de malware para infectar ordenadores y obtener datos bancarios, o bien los compran directamente a hackers dedicados a la obtención de las credenciales y datos bancarios necesarios para luego utilizarlos para estafar.

Un par de ejemplos de diversificación y especialización en la cadena de valor de la delincuencia online son aportados por la empresa de seguridad S21SEC. En el caso del blanqueo de capitales, este ha pasado a realizarse mediante cuentas robadas de casinos online, o agencias envíos de dinero online. Para ello hace falta contar con recursos de anonimato mediante *botnets*, que los ciberdelincuentes alquilan a sus nuevos socios. Otro caso es el de las bandas de Europa del Este dedicadas a la clonación de tarjetas en cajeros, que ahora ofrecen todos los aparatos necesarios para captar el pin y banda magnética y planchar una tarjeta nueva.

En cualquier caso, la BIT recuerda que la actividad delictiva no se reduce solamente a los datos bancarios. Hoy son muchos los datos personales que se almacenan en muchos sistemas y que una vez obtenidos pueden convertirse en dinero (espionaje, chantajes, presiones, etc).

Más aún, desde S21SEC se apunta que Internet cada vez está más presente en la actividad de la delincuencia en general, y aportan varios casos concretos a modos de ejemplo. Así, en las operaciones de fraude en banca online se necesita un "mulero" que reciba los fondos, en este nicho han entrado las mafias dedicadas tráfico de personas y explotación sexual. Otro ejemplo es que en los foros dedicados a la compraventa de malware y datos bancarios, ahora hay secciones enteras dedicadas a drogas y sus precursores, anabolizantes, fármacos controlados, armas de fuego y documentación

falsa. Todo está en venta, o bien la mercancía en sí misma o detallados videotutoriales para su fabricación.

¿Existe una conexión entre cibercrimen, ciberfraude y ciberterrorismo?

En palabras del representante de las FCSE, el ciberfraude es una actividad más del cibercrimen. En cuanto al ciberterrorismo, de alguna manera, también lo podíamos considerar parte del cibercrimen puesto que se trata de realizar actividades criminales, si bien merece un tratamiento diferenciado.

El ciberterrorismo puede referirse tanto a la utilización de Internet por parte de las organizaciones terroristas en los ámbitos de la propaganda, reclutamiento, financiación etc, como la posibilidad de ciberataques a las infraestructuras críticas de un país. En el primer caso es obvia la utilización y en el segundo existe la posibilidad y ya ha habido algunos ataques documentados.

Para prevenir estos supuestos en España tenemos el Centro Nacional de Protección de las Infraestructuras Criticas (CNPIC)

Ante pequeños ciberdelitos, ¿cómo las FCSE pueden dar una respuesta de forma coordinada con la Administración de Justicia?

Las estadísticas de denuncias de la Policía indican que aproximadamente el 60% de las denuncias de fraude son de una cuantía inferior a 400 euros (y el resto tampoco son cantidades elevadas). Por lo tanto, estos fraudes al estar considerados individualmente, en la mayoría de las ocasiones son tipificados como faltas, no delitos. Además las denuncias están diseminadas por varios juzgados de todo el país, con los problemas de competencia que ello conlleva y la falta de agilidad en las diligencias de investigación que son necesarias para la detención de los autores.

¿Cómo los proveedores de servicios que detectan ciberdelitos en distintos países pueden coordinarse con las FCSE y otros proveedores?

Dado que las acciones producidas por el malware y las amenazas en Internet no tienen fronteras, las FCSE deben estar coordinadas con los proveedores a través de acuerdos de colaboración y amparados desde una legislación que permita su actuación de una manera eficaz.

En opinión de TELEFÓNICA, el modelo antiguo, en el que las FCSE eran capaces de trabajar independientemente para la resolución de todas las acciones ilícitas, ha quedado obsoleto en un mundo cada vez más global, interconectado mediante la tecnología y en el que un terminal de última generación tiene una capacidad de proceso de varios órdenes de magnitud superior a los ordenadores más avanzados de hace veinte años. Así, las FCSE y los proveedores deben apoyarse mutuamente en beneficio de los ciudadanos y coordinados a través de un marco legal de actuación, en el que se respeten los derechos fundamentales de los ciudadanos y se permita identificar, perseguir y aplicar todo el peso de la ley a aquellos que utilizan Internet como una extensión natural de su forma delictiva de actuar.

Para TELEFÓNICA, afortunadamente el modelo internacional se está beneficiando cada vez más de los fuertes lazos de colaboración que se están estableciendo a nivel mundial entre las FCSE y los magistrados, siendo un ejemplo a citar el marco europeo legislativo y con unas FCSE coordinadas. En este sentido, desde la BIT se recuerda que existen diferentes instrumentos de cooperación policial internacional a través de Interpol, Europol, Sirene y también por medio de las relaciones bilaterales a través de los enlaces y agregados de los distintos países.

Las FCSE disponen de herramientas de inteligencia que rápidamente cruzan los datos de investigaciones diferentes y permiten saber por ejemplo que se trata del mismo autor/es. Para la investigación policial es fundamental la trazabilidad de las comunicaciones y que se guarden los datos de tráfico tanto por operadores de telecomunicaciones como por prestadores de servicios de Internet.

En cuanto a las IPs habría que distinguir cuando se trata de comunicación y cuando dato de carácter personal, ya que según la BIT de la Policía Nacional no tiene sentido dar protección de secreto de comunicaciones cuando el contenido de la comunicación, que es el dato verdaderamente protegido, ya se conoce. Otro tema importante para la investigación es el anonimato de las redes WiFi y los cibercafés.

En opinión de la BIT de la Policía Nacional, las empresas que prestan servicios en España deberían acogerse a la legislación nacional para facilitar los datos cuando se trate de hechos ocurridos en España. Pero cuando un ISP detecta ciberdelitos en distintos países pudieran plantearse varios supuestos:

- Si los ciberdelitos no tienen nada que ver los de un país con otro, debería presentar denuncia en los dos países.

- En el supuesto de que se trate de la misma actividad delictiva con víctimas en diferentes países también cabrían varias posibilidades, aunque la más lógica sería denunciar en el país en el que se presuma que están los autores o bien existan más víctimas. De esta forma se iniciaría una investigación policial y se pediría a los demás países los datos de víctimas y todas las gestiones necesarias, ya sea mediante intercambio de información policial o por comisión rogatoria según los casos. También cabe la posibilidad de abrir una investigación en cada país y que luego se intercambie la información policial. No obstante, para juzgar los hechos en el ámbito europeo existe la figura de la cesión de jurisdicción, de forma que se procura que juzgue el país que tiene más y mejores posibilidades de hacerlo.

¿Qué mejoras normativas son necesarias para la persecución del ciberfraude? ¿Es suficiente la reciente reforma del Código Penal?

La reforma debería extenderse a la Ley de Enjuiciamiento Criminal y adaptar los procedimientos de investigación y las medidas cautelares a las dinámicas comisivas específicas a través de Internet. Por ejemplo, ante ataques de denegación de servicio.

En el ámbito civil, para CFLABS, sería una gran ayuda que la LEC facilite y agilice la solicitud de medidas cautelares y el aseguramiento de prueba que a fecha de hoy son concedidos en casos sumamente específicos y con cuentagotas. Si nos permitimos ser más ambiciosos, resulta imprescindible un marco normativo que permita gestionar de forma cómoda y segura la prueba electrónica cuando ésta se encuentra más allá de nuestras fronteras.

Para LANDWELL-PWC, la principal mejora se refiere a la persecución de los delitos cometidos en servidores extranjeros, especialmente aquellos que han buscado la impunidad a través de: i) servidores específicamente diseñados para el cibercrimen; ii) servidores zombie; iii) proxy servers; iv) servidores en ciberparaísos; y v) medidas similares para eludir o dificultar la persecución

Las posibles soluciones que, en relación a la legislación nacional e internacional propone, son los procedimientos ágiles de auxilio internacional a la Justicia, el principio de legítima defensa internacional, que permita a los Estados actuar en servidores situados en ciberparaísos en el caso de ciberataques y el principio similar al *"hot pursuit".*

¿Quién asume la responsabilidad del fraude: los usuarios, los comercios, la entidad prestataria del servicio, la administración, etc.?

Precisamente el ponente de LANDWELL-PWC apunta que debería analizarse a cada actor para, caso a caso, definir legal y contractualmente sus obligaciones y las reglas de atribución de la responsabilidad.

- Particulares: responsabilidad en la custodia de las claves, negligencia, impericia, desinformación negligente, ausencia de protección (antivirus),
- Empresas, comercios, entidades financieras: medidas de seguridad, información a los clientes
- Prestador del servicio: medidas de seguridad, controles, información previa de la posible existencia del delito
- Administración: entorno legal adecuado, trasposición directivas y acuerdo internacionales, formación jueces y fiscales

La representante CIBERVOLUNTARIOS considera que la responsabilidad debe ser del prestatario del servicio o aplicación (empresa, administración…) y que, otra cuestión es que, se exija a los usuarios determinadas acciones o precauciones básicas para garantizar esa seguridad (ej: no revelar las claves a nadie, ser cuidadoso en la navegación y los datos personales proporcionados online, etc.)

Desde otro punto de vista, para TELEFÓNICA la responsabilidad del fraude la tiene el defraudador. Todos los elementos que el defraudador utiliza para desarrollar el fraude también están involucrados de manera involuntaria en el mismo, siendo generalmente el ciudadano el menos responsable y la primera víctima del fraude.

En su opinión, es tremendamente injusto acusar al ciudadano de fraude cuando ha sido engañado a través de una falsa oferta de un producto software (aplicación) que instala en su dispositivo móvil sin hacer más verificaciones sobre su bondad o veracidad y a través de la que pueden llegar a realizarse delitos de fraude. Pero, a su vez, también es injusto acusar a una operadora que provee un servicio de comunicación al ciudadano según una regulación legal claramente establecida de la responsabilidad de un fraude.

En este caso se debe hablar de perjudicados, en plural. El primer perjudicado es el ciudadano, que ha sufrido en su persona y a través de un dispositivo de su propiedad una elaborada y técnicamente muy compleja artimaña que le ha situado en el objetivo de un fraude.

Pero, igualmente, otro de los perjudicados es la operadora, ya que se ha utilizado un servicio que presta al ciudadano y sobre el que ha volcado toda su buena intención, conocimiento y respeto a la ley para prestar un servicio público.

La ley es clara en estos asuntos y siempre trata de proteger al más desfavorecido: el ciudadano que ha sido víctima de fraude a través de un engaño, muy elaborado en estos casos.

¿Cómo está respondiendo la industria a la demanda de seguridad de las pymes y de las grandes empresas?

Para S21SEC la seguridad está en continuo cambio, por lo que la única forma de dar respuesta que tiene la industria de la seguridad es la investigación e innovación constante. Los ataques no cesan, y hay que estar alerta, ser siempre proactivos y responder con inmediatez. Las pymes y las grandes empresas pueden cubrir sus necesidades mediante una gestión integral de su seguridad y una puesta en marcha de una política preventiva de seguridad o solicitar productos y servicios reactivos concretos. Algunas soluciones que ofrecen las empresas de seguridad son la protección contra el fraude, cumplimiento normativo, concienciación y formación, gestión de logs y auditorías de seguridad entre otros.

En este sentido, TELEFÓNICA añade que la industria ha identificado la seguridad tanto de las pymes como de las grandes empresas como un nicho de negocio en crecimiento. Por ello, tanto las compañías privadas dedicadas a la seguridad tecnológica como compañías de servicios, incluyen la seguridad dentro de su cartera de productos o como complemento a servicios específicos.

Para TELEFÓNICA existen dos modelos de acercamiento diferente según cada caso. El acercamiento a la pyme se realiza a través de la paquetización de la seguridad de forma conjunta a los productos y servicios ofrecidos, frente al acercamiento a las grandes empresas, en el que se conjugan los servicios de auditoría de seguridad específicos, acompañados de la implantación de modelos de seguridad complementarios a los servicios específicos contratados por estas compañías.

En relación a la prueba electrónica, CFLABS considera que la industria y, sobre todo los diferentes actores jurídicos que intervienen, han respondido durante la última década de una forma espectacular en nuestro país. Hace tan sólo una década los abogados evitaban tener que recurrir al uso de la prueba electrónica y los magistrados no sabían muy bien qué hacer con ella. Hoy por hoy es una prueba más, con metodologías establecidas y compartidas por el sector privado y los FCSE y con magistrados y fiscales formados en el uso de las mismas.

Tanto la industria como las administraciones están colaborando y prestando gran esfuerzo en minimizar el impacto de los riesgos y generar confianza en los nuevos modelos. Pero la ciberdelincuencia y las amenazas de seguridad continúan evolucionando y, en opinión de S21SEC, todos tenemos que seguir trabajando.

¿Cómo mejorar la adopción de buenas prácticas y mejorar el nivel de seguridad y privacidad en las empresas?

Para S21SEC la concienciación en seguridad de la información es la "asignatura pendiente" de la mayoría de las empresas.

Desde su punto de vista, lo mismo que la formación en prevención de riesgos laborales se considera básica para la seguridad de los trabajadores, la formación en "prevención de riesgos digitales" es la base para la seguridad de la información. Esto se debe a que la mayor parte de los incidentes de seguridad que se registran son provocados por un descuido o desconocimiento del procedimiento correcto a seguir en el uso de las TIC. Por tanto, la formación de todos los trabajadores para adquirir unas "buenas prácticas" de seguridad, junto con la aplicación de una adecuada política de seguridad corporativa, son los dos pilares para minimizar los incidentes de seguridad y su impacto.

En algunos casos – por ejemplo la prueba electrónica – desgraciadamente no hablamos de "mejorar" esa concienciación sino de "crearla" de la nada. Si bien existen casos puntuales donde el valor de determinadas transacciones electrónicas resulta obvio y son debidamente tratadas, en general hay muy poca aceptación de las líneas de prevención en este ámbito.

Para la empresa CFLABS, los servicios destinados a minimizar el anonimato digital en la empresa y a lograr una auténtica "trazabilidad forense" son, hoy en día, sólo apreciados por un selecto y reducido grupo de sectores

Más allá, desde LANDWELL-PWC se apuntan mejoras a través de códigos éticos y normas de uso de los recursos TIC, la aplicación del régimen disciplinario a los casos de infracción, un canal de denuncias interno y externo, el reconocimiento de los comportamientos ejemplares, y la formación online.

¿Cuál es la percepción de los ciudadanos respecto al fraude online?

El fraude tiene dos consecuencias directas sobre los usuarios: en primer lugar, la pérdida económica tangible en caso de que el ciberdelincuente consiga su propósito; en segundo lugar la posible pérdida de confianza que los internautas pueden experimentar tras ser

víctimas de una situación de fraude. Este segundo efecto, quizás menos nombrado que el primero, no es en absoluto trivial e incide en el desarrollo y consolidación de la Sociedad de la Información.

Según los datos del Observatorio de la Seguridad de la Información de INTECO, un 4% de los internautas declaran haber sufrido un perjuicio económico víctimas de un fraude online (aunque la mayoría son de una cuantía económica no muy elevada, por los que muchas veces no se denuncian a la FCSE: más del 80% de los casos declarados, ni siquiera es delito, sino falta, al estar por debajo de los 400€)

Los casos de fraude no afectan al nivel de confianza de los usuarios y su incorporación a los servicios económicos de Internet. Su percepción es que Internet es cada día más seguro. La consideración de que el equipo personal está razonablemente protegido presenta una evolución creciente.

Los estudios de INTECO arrojan como resultado que el fraude online es más una "barrera de entrada" para los no usuarios que un "impulso de salida" para los usuarios de banca y comercio electrónico. Las tasas de abandono son ciertamente minoritarias, incluso entre los ciudadanos que han experimentado un perjuicio económico, lo que supone un indicio de que ciertos servicios de Internet – en especial la banca electrónica – son difícilmente sustituibles para sus usuarios. Se debe tener en cuenta este indicador, en tanto en cuanto constituye un indicio muy fiable del nivel de e-confianza de la ciudadanía.

Se observa una evolución positiva de la percepción del usuario, el cual no sólo declara que está cada vez mejor protegido (el uso de tecnologías o servicios de seguridad de la información es cada vez más alto: instalación de software antimalware, firewalls, antispam), sino que cada vez es más capaz de detectar posibles amenazas (como el phishing) o intentos de estafa basados en ingeniería social. No obstante conviene seguir insistiendo en otras tecnologías como la recuperación de datos, cifrado de información, etc., que aumentan más aun el nivel de seguridad.

CIBERVOLUNTARIOS manifiesta de la mano de las redes sociales se ha incorporado un tipo de usuarios no habituados al uso y manejo de herramientas tecnológicas. La cercanía del entorno en el que se mueve les hace sentir una falsa seguridad, propicia para las infecciones de malware y el ciberfraude. Por otra parte, también preocupa la variedad y versatilidad de los ataques.

Su opinión es que – aunque se produzcan grandes fallos como los que últimamente están en los medios por el robo de datos en grandes compañías – la industria a nivel técnico está respondiendo bien y a un alto nivel. Se va a más en las medidas seguridad que se toman: encriptación de datos, contraseñas temporales que se trasmiten instantáneamente a terminal móvil y e incluso ponen en valor tecnologías como el NFC (*Near Field Communication*) – tecnología inalámbrica, de corto alcance y alta frecuencia que permite el pago a través de móviles de ultima generación acercando el terminal cerca del punto de venta.

Sin embargo, en la comunicación, los propios internautas perciben una apuesta por parte de la industria hacia la política del miedo, enfocada en las herramientas (antivirus, firewall). Se sienten impotentes al tener que comprar productos cuya licencia tienen que renovar cada año y que además, si hay algún problema, no garantizan que el proveedor del servicio se hará responsable. En este sentido, exigen efectividad, y hoy por hoy no están satisfechos.

Además, piensan que ese tipo de comunicación, basada en la política del miedo, busca la venta de productos y no la corresponsabilidad, y sienten que hace un flaco favor a la gente que todavía se está incorporando al uso de la tecnologías, especialmente a las personas mayores.

Por último, CIBERVOLUNTARIOS reivindica que las administraciones tienen mucho que avanzar, y que tienen que apropiarse de la visión de que hay que ponerse al nivel de quien no sabe ni usa las TIC habitualmente y no al contrario. Consideran que herramientas como el DNI electrónico y el certificado digital son difíciles de usar y que la duplicidad (DNI-e y certificado digital) confunde y no da confianza a la población. Aparte de sentir que los ciudadanos no conocen los servicios que ofrece el DNIe y lo que influye en que no se use demasiado.

¿Cómo mejorar de la concienciación y la cultura de la seguridad de los usuarios desde la industria, administraciones y la sociedad civil? ¿A través de qué acciones, en qué canales y formatos?

Todos los ponentes coinciden en que es importante que todos los implicados unan esfuerzos para evitar que el fraude suponga un freno al desarrollo de la Sociedad de la Información.

Desde la BIT de la Policía Nacional se percibe una cierta falta de cultura de seguridad en el uso de Internet entre los ciudadanos, no solo en los aspectos técnicos, sino tampoco como en lo que debe ser un uso racional y prudente respecto de los datos personales en Internet. Debe formarse a los niños en diferentes aspectos de la seguridad necesaria en un espacio virtual que va a formar parte de su vida. Para la Policía, una asignatura como educación para la ciudadanía, ya sea transversal o no, debiera ayudar a formar “ciudadanos digitales” que forman parte de la sociedad de la información que nos ha tocado vivir.

Desde la industria, en este caso TELEFÓNICA, existen dos formas complementarias de concienciación. En primer lugar, la inclusión de servicios de seguridad en los servicios y productos destinados a los ciudadanos. El ciudadano no debe ver la seguridad como un “extra” que le cuesta más dinero y cuyos efectos no tiene claramente definidos. Los servicios siempre deben incluir la seguridad como parte indisoluble de los mismos, promoviendo en la oferta de las empresas una competencia (paralela a la del producto) consistente en la seguridad del propio producto o servicio.

Y, en segundo lugar, la formación. Es imposible concienciar sin formar. La formación debe ser multinivel, cubriendo a todas las edades y dirigida hacia todas las franjas de la

población, en la que se describan y expliquen los riesgos de una forma no negativa y los medios existentes al alcance de cualquier persona para combatirlos.

LANDWELL-PWC coincide en algunas de estas medidas de sensibilización y plantea las siguientes acciones: campañas de concienciación, decálogo de buenos usos de Internet y decálogo de malos usos de Internet, y descripción de casos reales, recomendaciones de medidas preventivas, guías para padres y materiales para profesores, o acuerdos con productoras audiovisuales para incluir mensajes en películas y series, entre otras. Plantea que los canales idóneos sean las redes sociales, blog, medios de comunicación colaboradores, webs de las FCSE, y en formatos atractivos para los internautas como guías, videos virales, comics, videojuegos, salvapantallas y fondos de escritorio.

CIBERVOLUNTARIOS considera que esta labor debe realizarse desde una política de trabajo multiactor, en el que el usuario deje de ser un mero receptor de políticas de seguridad para ser un actor en ellas. Promover una alfabetización informacional en este sentido es la base y la puerta para que el ciudadano posteriormente pueda contribuir, ser parte activa, en la responsabilidad con respecto a su seguridad, así como en otros aspectos, como por ejemplo, sus derechos en Internet, su identidad, su privacidad, etc

Declaran que la primera acción es deshacerse de la cultura del miedo y sustituirla, como hemos comentado antes, por la de una alfabetización informacional y tecnológica que empodere a los ciudadanos y los haga corresponsables. Los jóvenes pueden ser uno de los canales más importantes para trabajar en ese intercambio seguridad, trabajo colaborativo, e-confianza, prevención, redes… Y que hay que romper mitos, sobre todo en el ámbito de las personas mayores, muchos de los que están les gusta navegar y se sienten seguros, pero esto no se comunica.

Añaden que los formatos han de ser muy variados: desde lo más tradicional (cursos, charlas, talleres, eventos) pasando por la necesidad de atención y respuesta online inmediata hasta temas de creación de redes colaborativas, videos participativos, tutoriales a través de videos explicativos, entre otros.

Desde INTECO se insiste en que hay que promover una cultura de la seguridad y de la privacidad “más sencilla e intuitiva”, acudiendo cada vez más al sentido común. Lo mismo que la tecnología es cada vez más transparente, la seguridad también ha de serlo, y cuanto más implícita sea dicha seguridad en la tecnología y los servicios, más viable será que el ciudadano confíe en dicha tecnología y servicios. Es una labor de repetición al mismo nivel que desde otras administraciones como la DGT o Sanidad se insiste en ciertos riesgos y se lanzan mensajes para mejorar el impacto.

Precisamente este organismo trabaja este aspecto con guías, alertas, boletines, blogs, avisos web y avisos en redes sociales, etc. buscando formatos que consigan aglutinar en pequeña píldoras (videos, animaciones, juegos, etc.) un mensaje de concienciación, recomendación o prevención, con una componente interactiva que facilite la asimilación del mensaje y el aprendizaje. En este sentido, por ejemplo INTECO tiene varios perfiles publicados en redes sociales y a través de los mismos transmite gran parte de su información y actividad con el fin de ser lo más interactivos y virales posible.