EUSKO JAURLARITZA
GOBIERNO VASCO

nº 51
Marzo de 2015

Aurrera!

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

- Nuevas formas de trabajar
  Pág. 2
- Ciberseguridad: ataques dirigidos denominados APT (Ataques Persistentes Avanzados)
  Pág. 6
- Alboan:
  Estandarización de las encuestas electrónicas (Eustat)
  Pág. 10
- Breves:
  Telefonía móvil: «modo avión»
  Primeros móviles con Ubuntu
  Pág. 12

A medida que incorporamos las Nuevas Tecnologías a nuestra vida, la forma de trabajar también evoluciona. Tanto es así que hoy en día parece imposible realizar nuestro trabajo sin correo electrónico, sin dispositivos móviles, etc. En el primer tema de este Boletín Aurrera, reflexionaremos sobre las Tecnologías de la Información y Comunicaciones (TIC), las nuevas generaciones de jóvenes que se incorporan al mercado laboral y cómo ello está afectando a la forma de trabajar presente y futura.

Todos sabemos que el mundo de las Nuevas Tecnologías está en continuo avance, y el mundo de la seguridad informática no es una excepción. Tal es así que cada día surgen nuevas formas de atacar los sistemas de información. La última tendencia en el mundo de la ciberseguridad son los llamados Ataques dirigidos APT (siglas en inglés de «Ataques Persistentes Avanzadas»). En el artículo que hemos elaborado en esta ocasión os explicamos sus principales características.

Para el apartado «*Alboan*» hemos contado con la colaboración del Eustat. Los responsables de este Organismo Autónomo nos presentan, en este caso, las conclusiones del trabajo que han realizado durante los últimos años para mejorar la estandarización de las encuestas electrónicas, lo cual les ha permitido reducir los costes de desarrollo y mantenimiento del software de los cuestionarios, así como mejorar la calidad de los mismos. En el artículo veremos cómo lo han conseguido.

Seguro que en más de una ocasión a la hora de despegar en un avión habéis oído la famosa frase «por favor, apaguen sus teléfonos móviles». Pues bien, según parece, la EASA (Autoridad Europea de la Seguridad Aérea) ha abierto el camino para que podamos viajar con nuestros dispositivos electrónicos sin necesidad de apagarlos. Tienes más información en el apartado «Breves».

Como segunda noticia de este apartado, hemos incluido una relacionada con el mundo del Software Libre. En ella os informamos de la salida al mercado del primer teléfono móvil que funcionará con Ubuntu. Para conocer todos los detalles del mismo, no os perdáis la noticia que hemos elaborado.

Nuevas formas de trabajar

Puede que la era de las «oficinas tradicionales» esté llegando a su fin. De hecho, hoy en día los trabajadores de muchas empresas emergentes ya no tienen que cumplir estrictos horarios y acudir diariamente a su oficina, gracias, principalmente, a que las Nuevas Tecnologías permiten trabajar con cualquier dispositivo móvil desde cualquier lugar.

Han nacido y crecido en plena expansión de la tecnología y hoy conviven con ella en la palma de la mano. Tienen entre 18 y 33 años. Se informan, comparten conocimiento, gustos, opiniones, e incluso, consumen a través de Internet y de las redes sociales, a cualquier hora y desde cualquier lugar, en **movilidad**. Son «seres sociales» que viven permanentemente conectados: son los ***millennials***; también conocidos como la *Generación Y* o *Net Generation*, los cuales supondrán en 2025 el 75% de la fuerza laboral del mundo, pronostica la consultora Deloitte.

Los *millennials* se han educado en un mundo donde Internet es ya algo omnipresente; procesan la información de manera diferente a otras generaciones; disfrutan de una nueva forma de comunicación bidireccional de la mano de las redes sociales, son participativos y digitalmente expertos. En definitiva, tienen una particular forma de entender/utilizar la tecnología y la conectividad, las cuales se esperan encontrar o poder utilizar también en el trabajo.

Según destaca Deloitte en el informe **Grandes demandas y expectativas** sobre los *millennials*: «*Ya están emergiendo como líderes en tecnología y otras industrias y quieren trabajar para organizaciones que fomenten el pensamiento innovador, el desarrollo de sus habilidades, y hagan una contribución positiva a la sociedad*».

La gran oportunidad que representa escuchar a esta generación debería influir tanto en la industria como en los servicios públicos para adaptarse a los nuevos desafíos, pues son estas personas las llamadas a escribir el futuro con su optimismo, energía y carácter innovador.

«Los *millennials* supondrán en 2025 el 75% de la fuerza laboral del mundo»

LA TECNOLOGÍA

Todos somos conscientes de que los entornos de trabajo están cambiando. Las TICs, la nube, los *smartphones* y las *tablets* han «derribado» los muros de la oficina: espacios de trabajo virtuales, trabajadores en movilidad, equipos cuyos miembros no están en el mismo lugar… Y, de otro modo, la necesidad de implementar medidas de seguridad laboral de acuerdo con las obligaciones legales y una mayor concienciación y disposición en el mundo empresarial hacia entornos de trabajo seguros y personas felices, siendo ésta una máxima en las políticas de retención del talento. Por supuesto, las **Administraciones Públicas** no son una excepción a esta tendencia, y ya se multiplican los proyectos de Teleasistencia, Teletrabajo[1], *apps* para interactuar con la ciudadanía…

El último informe de la compañía Randstad sobre la gestión y fidelización del talento revela que para las trabajadoras y trabajadores menores de 40 años, el salario es uno de los factores que más valoran para elegir una empresa en la que trabajar,

DICCIONARIO

[1] **Teletrabajo:** información sobre el Proyecto de Teletrabajo del Gobierno Vasco:

«*DECRETO 92/2012, de 29 de mayo, por el que se aprueba el Acuerdo sobre la prestación del servicio en la modalidad no presencial mediante la fórmula del teletrabajo por el personal empleado público de la Administración General de la Comunidad Autónoma de Euskadi y sus Organismos Autónomos*» (BOPV nº 111, de 7 de junio de 2012)

Para conocer más aspectos y características del Teletrabajo podéis consultar *El Libro Blanco del teletrabajo en España* (junio 2012, Fundación Masfamilia)

www.teledislab.es/descargas/libroblancoteletrabajoespana.pdf

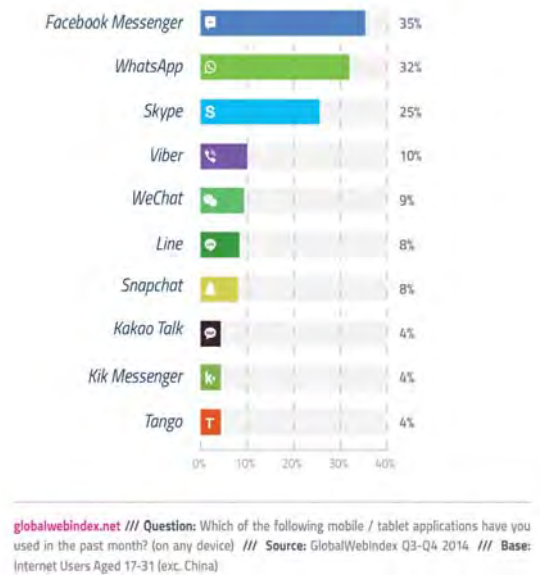
pero también valoran la **utilización de tecnologías punteras**. Igualmente, la atmósfera laboral y la conciliación entre el trabajo y la vida privada son dos de los asuntos capitales a la hora de decantarse por una compañía o un organismo público.

El citado estudio destaca también que una de las prioridades en el denominado *employer branding* es facilitar la conciliación. «*La felicidad del empleado en su puesto laboral y la ausencia de preocupaciones que influyan negativamente en su vida privada repercuten de manera directa en su productividad*», resalta. Un último apunte: Tecnología y Electrónica son, un año más, los sectores más deseados para trabajar.

Y es que tener como trabajadores personas satisfechas, orgullosas del lugar en el que trabajan, redunda de forma positiva en la productividad de la organización. Según **Great Place To Work**, «*los excelentes lugares para trabajar logran los objetivos de la organización inspirando, comunicando y escuchando. Tienen empleados que dan lo mejor de sí cuando se les agradece, se los desarrolla y se los cuida*».

En este mundo globalizado, las empresas, públicas o privadas, no pueden despilfarrar uno de los recursos más valiosos y escasos: **el tiempo**. Las relaciones entre los empleados/as y empleadores

Sistemas de mensajería que utilizan los *Millennials*



globalwebindex.net /// **Question:** Which of the following mobile / tablet applications have you used in the past month? (on any device) /// **Source:** GlobalWebindex Q3-Q4 2014 /// **Base:** Internet Users Aged 17-31 (exc. China)

deben buscar nuevas actitudes que posibiliten la generación de valor para ambas partes. Esa flexibilidad produce numerosos beneficios para el trabajador/a y para los equipos de trabajo con los que interactúa. También se ven beneficiadas las empresas y, por supuesto, el conjunto de la sociedad.

«Estamos ante un auténtico cambio cultural en el modo de trabajar, un cambio que no es tecnológico sino facilitado por la tecnología»

Y si el entorno tecnológico y demográfico cambia, las relaciones laborales también deben adaptarse a las nuevas circunstancias. Conceptos como ecología, diversidad, internacionalización, inclusión, género, **movilidad**, ciudades inteligentes[2], información, transparencia o **tecnología** adquieren una dimensión empresarial de la mano de la sostenibilidad. Indagar en estas nuevas formas de trabajar resulta imprescindible para lograr el crecimiento económico sostenible que genere empleo duradero y de calidad.

Hoy en día, gracias a Internet todas las personas están conectadas, están *on-line*. Es más, gracias a las Nuevas Tecnologías es perfectamente viable gestionar una empresa a través de ellas sin estar físicamente en la oficina.

Millennials, tecnología, conectividad, talento, flexibilidad, conciliación, productividad, eficiencia, ¿es necesario en este nuevo panorama una nueva forma de trabajar? Lo que está claro es que ya no estamos en el mismo escenario que años atrás. El contexto ha cambiado, y si nosotros no cambiamos, y sobre todo, nuestra forma de pensar, estamos condenados a la «obsolescencia». Es necesario comenzar a interiorizar esa **New Way to Work**, o «nueva forma de trabajar» basada en **la movilidad**, **la flexibilidad** y **la eficiencia**, que beneficia tanto a los *millennials* como a «inmigrantes» digitales. Todo lo cual acabará beneficiando y facilitando la vida a todas las personas trabajadoras de la entidad, a la propia empresa y, en definitiva, a la sociedad en general.

Esta nueva forma de trabajar ya se está convirtiendo en una iniciativa de investigación del mercado, diseñada para ayudar a las organizaciones a entender el impacto de los «equipos de trabajo virtuales», así como las

DICCIONARIO

[2] **Ciudad inteligente**: es la traducción del término en inglés *smart city*.

La «ciudad inteligente» a veces también llamada «ciudad eficiente», se refiere a un tipo de desarrollo urbano basado en la **sostenibilidad** que es capaz de responder adecuadamente a las necesidades básicas de instituciones, empresas, y de los propios habitantes, tanto en el plano económico, como en los aspectos operativos, sociales y ambientales, es decir, que disponga de un desarrollo económico-ambiental durable y **sostenible**, una gobernanza **participativa**, una gestión prudente y reflexiva de los recursos naturales, y un buen aprovechamiento del tiempo de los ciudadanos.

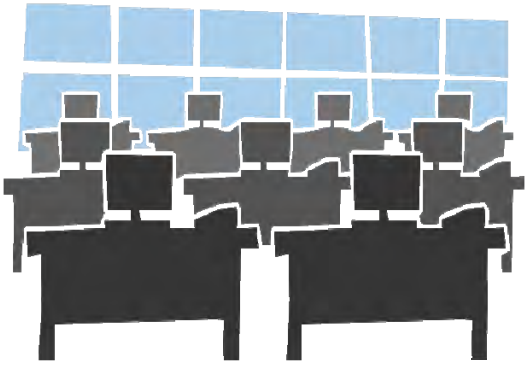
[Fuente: Wikipedia]

Para más información ver el artículo titulado *Datos masivos (Big Data)* del boletín Aurrera nº 44 (junio de 2013).

www.euskadi.eus/informatica

mejores políticas para llegar a ser una empresa comprometida con el mundo actual.

Sin embargo, este **cambio de cultura o filosofía** no está exento de amenazas y riesgos que es necesario evaluar. Desde un punto de vista externo, por ejemplo, la principal amenaza a la que debe enfrentarse la organización es la dinámica



del entorno que exige **recortes presupuestarios** y en el que prima el **corto plazo** frente al largo plazo. El miedo a invertir en tecnología puede llegar a priorizar lo coyuntural frente a lo estructural. La herencia recibida de la **época industrial** es otra clara amenaza a las nuevas formas de trabajar y comunicar.

Sin embargo, las oportunidades que puede aprovechar la organización son múltiples, comenzando por el **efecto multiplicador de las TIC** en el alcance de la actividad de la entidad. La diferenciación frente a la competencia es otra ventaja competitiva para la empresa, que incide directamente en su rentabilidad, o en el crecimiento del volumen de negocio. La anticipación y adaptación a cambios en normativas legales también se consensuó como otra gran oportunidad, que genera flexibilidad transversal en la organización. Evidentemente, cualquiera de estos aspectos también es extrapolable a la propia Administración Pública, donde las medidas de control presupuestario, la apuesta por la sostenibilidad y la conciliación, etc., se han convertido en una máxima para ellas.

COMUNICACIONES UNIFICADAS

Evidentemente **la tecnología** debe ser el catalizador que nos ayude a evolucionar hacia esa nueva forma trabajar sin problemas, y desde donde queramos o necesitemos. Si le sumamos el absolutamente necesario (y clave del éxito) **cambio cultural** necesario en las citadas organizaciones, tendremos el coctel perfecto para abordar lo que está pasando en los modos en que las personas se relacionan personal y laboralmente.

Llegados a este punto, habría que preguntarse cómo esa función catalizadora de la tecnología se traduce en soluciones a las nuevas problemáticas que se plantean. Si se utiliza una visión simplificadora, el camino vendrá dentro de lo que genéricamente se denomina «**Comunicaciones Unificadas**»[3], término excesivamente utilizado, y que cada fabricante interpreta de una manera distinta, pero que, sin embargo, puede ser resumido en el uso de unas pocas **funcionalidades**:

- **Número único y dispositivo preferido**. ¿Cuántas veces hemos intentado localizar a alguien primero en su teléfono fijo, luego en su móvil…? ¿Cuantos minutos se pierden al día intentando localizar a alguien por distintos medios? Esta funcionalidad permite a cada persona usuaria determinar cómo quiere que la localicen, independientemente de donde se encuentre, así como en qué dispositivo de comunicación. Los demás usuarios sólo tienen que saber un número, y serán nuestras reglas de enrutamiento las que determinen el resto.

- **Presencia**. Tenemos que ser capaces de determinar en cada momento cuál es nuestro nivel de disponibilidad a ser localizados, ya sea en función del horario, de nuestra actividad, o de otros factores.

DICCIONARIO

[3] **Comunicaciones Unificadas:** para más información, podéis consultar el artículo *Comunicaciones unificadas* que se publicó en el Boletín Aurrera nº 46 (diciembre 2013).

www.euskadi.eus/informatica

- **Buzón único**. Esta funcionalidad nos permite disponer de un único buzón dónde centralizar todos los mensajes, puesto que ¿tiene sentido disponer de un buzón para voz en el teléfono fijo y otro en el móvil, por ejemplo?

«El trabajo ya no es un lugar o un horario, sino una actividad»

- **Mensajería instantánea**[4]. No siempre es necesario realizar una llamada de voz para comunicar algo a alguien. Quizá lo que mejor explica esta funcionalidad es la extraordinaria explosión que han tenido aplicaciones de este estilo, tanto en el ámbito personal como en el empresarial.
- **Aplicaciones móviles**. En un mundo en absoluta movilidad e «hiperconectado», es necesario disponer de las mismas herramientas tanto si estoy en la oficina como en cualquier otro sitio, y son las aplicaciones móviles las que permiten gestionar esto.
- **Herramientas de Colaboración y Conferencias vía web**. Si los equipos de trabajo son cada vez más «virtuales», cada persona se encuentra en un sitio distinto, etc., proveer herramientas que permitan reuniones de esos grupos es vital. Con toda seguridad, este es uno de los elementos clave y que merece un poco de detalle, prestando especial atención no sólo a la herramienta en si, sino al uso que se hace de la misma. De hecho, son varios los **consejos** que podemos dar para hacer un uso eficiente de estas herramientas para evitar las frustraciones que muchas personas sufren a la hora de usar estas tecnologías:
  - Convocar una sesión de colaboración (bien sea de audio o web) sólo cuando sea necesaria, no es bueno hacerla para todo. Hay veces en que con un correo, o simplemente con una llamada, se resuelve un problema. Conclusión: no es bueno abusar de las reuniones.
  - Utilizar una herramienta tipo «Agenda Corporativa» para que todas las personas convocadas la tengan anotada (no hay que fiarse de la memoria). Funcionalidades, como pueden ser el **número único** y el **estado de presencia** son fundamentales para todas las personas que trabajan en movilidad.
  - Convocar sólo a aquellas personas que son necesarias y puedan aportar algo. De hecho, una reunión no será más productiva porque haya más asistentes colaterales al tema.
  - Una sesión debe durar lo que pone en la convocatoria, ni un minuto más, y se deben tratar los temas para los que fue convocada (en este sentido, tener un orden del día es fundamental). Si en vez de una hora puede durar media, mejor (las personas asistentes lo agradecerán).
  - Configurar el sistema para que sea éste quien llame a las personas convocadas, o bien, sean ellas mismas las que llamen en función de la obligatoriedad de la asistencia.
  - Como una imagen vale más que mil palabras… no tengas dudas a la hora de utilizar durante la reunión herramientas de *WebCollaboration*, ya que son altamente eficaces.

CAMBIO DE PARADIGMA

Está claro que el paradigma de las empresas tradicionales está cambiando. Como consecuencia de ello, se está eliminando la red laboral tradicional por una nueva en la que impera la **flexibilidad horaria y la movilidad**.

Estamos ante un auténtico cambio cultural en el modo de trabajar, un cambio que no es tecnológico sino facilitado por la tecnología, y que quizá se resuma en una frase, «*El trabajo ya no es un lugar o un horario, sino una actividad*». ❑

DICCIONARIO

[4] **Mensajería instantánea**: los clientes de mensajería instantánea más utilizados en el pasado fueron ICQ, Yahoo! Messenger, Pidgin, AIM (AOL Instant Messenger), Google Talk (sustituido hoy en día por Hangouts) y Windows Live Messenger (integrado hoy en día en Skype).

Actualmente la mensajería instantánea ha dado un vuelco hacia las aplicaciones móviles, aplicaciones multiplataforma, o directamente servicios web que no necesitan de ninguna aplicación para poder funcionar. Tienen especial relevancia Facebook_Messenger, Skype, Line, Hangouts, Telegram y Whatsapp.

Así mismo, empiezan a aparecer nuevas herramientas de **colaboración social** basadas en WebRTC (como puede ser, entre otras, *Circuit* de la empresa Unify) la cuales incorporan voz, vídeo, compartición de pantalla, mensajería instantánea e intercambio de ficheros, en un mismo interface para una más ágil, sencilla y natural comunicación.

Ciberseguridad: ataques dirigidos denominados APT (Ataques Persistentes Avanzados)

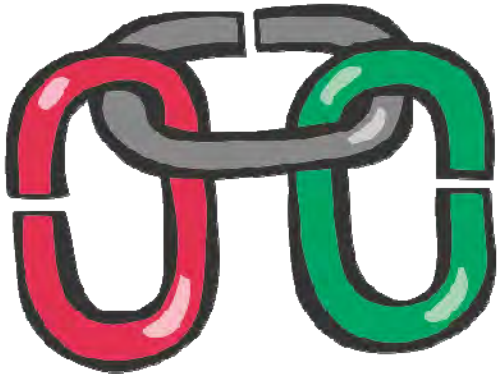
Las predicciones en el área de la ciberseguridad para este año 2015 apuntan a un aumento de los ataques dirigidos denominados *Ataques Persistentes Avanzados* (APT, en inglés), vamos a intentar dar un poco de luz sobre este tema.

DICCIONARIO

[5] **Ciberespacio:** es un término que popularizó la novela *Neuromante* escrita por William Gibson en 1984; no se debe confundir los términos Internet y Ciberespacio, con este último se hace referencia a un intangible al que podemos acceder todos, a través de una computadora, y que no tiene traslación con un lugar físico específico.

Fuente: http://es.wikipedia.org/wiki/Ciberespacio

En el ámbito de la ciberseguridad, entendiendo ésta como la gestión del riesgo en el ciberespacio[5], la tendencia, para este año 2015, es un aumento considerable de los ataques conocidos con el nombre de APT: término de origen militar, que se acuño por primera vez en el año 2006 en Estados Unidos, y que es la denominación con la que se conoce a las *Ataques Persistentes Avanzados*.



ESCENARIO ACTUAL

Las vulnerabilidades y fallos de seguridad son nuestro pan de cada día en los desarrollos de Tecnologías de la Información y de las Comunicaciones (TIC), favorecidas por varias razones: el lanzamiento de productos y versiones no probados suficientemente, la baja calidad de los productos desarrollados, la propia complejidad de los mismos, etc.; estas vulnerabilidades se asumen como algo natural, que es subsanado por las actualizaciones (en algunos casos llamadas «parches») que se lanzan a posteriori, y que corrigen muchos de estos fallos (en el boletín AURRERA nº 50 de diciembre de 2014, dentro del artículo titulado *Comprometiendo aplicaciones Web: XSS*, hablamos de *Cómo conseguir una web segura*); existen vulnerabilidades que son informadas por los fabricantes del producto o servicio para que sean corregidas, pero también es cierto que hay vulnerabilidades que son advertidas por terceros sin que quien ha lanzado el producto o servicio sea consciente de ellas, y, si este tercero actúa de mala fe puede poner en graves problemas a las organizaciones que utilizan ese producto/servicio, y que contiene un fallo de seguridad.

ADVANCED PERSISTENT THREATS

APT son las siglas de las palabras inglesas *Advanced Persistent Threats* (Ataques Persistentes Avanzados), que se refieren a un tipo de ataque que tiene unas características muy específicas, como son la duración en el tiempo, utilizar vulnerabilidades desconocidas oficialmente, y estar dirigidas contra objetivos concretos; vamos a ver qué significan las tres palabras que componen su nombre:

- **Ataque (*threat*)**: como explicamos en el número anterior del boletín AURRERA! una **vulnerabilidad o fallo de seguridad** no es sino una debilidad de un sistema de información (o de sus procedimientos de seguridad, o de sus controles internos, etc.) que podría ser utilizada para producir un incidente de seguridad, de tal modo que la posibilidad de que una vulnerabilidad se explote constituye una **amenaza y es posible que se realice un ataque** (si esta amenaza se materializa sobre un activo/recurso del sistema de información o relacionado con este es cuando el incidente de seguridad es un hecho, se produce un ataque, y puede conllevar un **daño)**. Como se ha comentado anteriormente, los ataques APT suelen utilizar vulnerabilidades que se desconocen, con lo cual las medidas de seguridad consideradas «tradicionales» no tienen el efecto esperado en estos casos.
- **Persistencia (*persistent*)**: esta es una característica relacionada con la intensidad, la firmeza y el empeño, que no tiene por qué estar

relacionada con la duración del ataque, por ejemplo, un ataque por denegación de servicio (ataque DoS[6]) también puede durar en el tiempo, y no tiene que ser una ataque del tipo APT; a lo que se refiere la palabra persistencia es a que existe una fase de estudio y análisis del objetivo (fase de preparación inicial) que tiene vital importancia en la consecución del ataque (en función de los resultados de esta primera fase el ataque puede llegar a tener éxito), y que este ataque es capaz de estar activo o latente sin ser detectado; como por lo general esta clase de ataques suelen ser de cierta importancia, se dedican mucho tiempo y recursos para conseguir los objetivos marcados. El ser persistente en el tiempo implica que el ataque no sea descubierto por los administradores del sistema atacado, para ello suelen lanzar otros tipos de ataques que saben que serán detectados, para, de este modo, encubrir el ataque APT.

- **Avanzada (*advanced*)**: esta característica indica una capacidad técnica alta por parte de las personas atacantes, y, a su vez, que se exploten vulnerabilidades desde un punto de vista novedoso y altamente tecnificado; esto implica que los métodos tradicionales de detección de ataques basados en «firmas», tal y como trabajan los antivirus actuales (una «firma» reconoce una cadena de ceros y unos en cierto contexto y lanza una alarma, debiéndose actualizar estas firmas de una manera periódica), no funcionen en estos casos. Por ello, las personas que pertenecen a estos grupos de cibercriminales suelen estar altamente cualificadas. Por lo general, estos ciberdelincuentes suelen ser personas que pertenecen a organizaciones delictivas (grupos organizados especializados) e incluso a gobiernos, que suelen disponer de recursos económicos para acometer estas acciones.

«El modelo de seguridad tradicional no sirve para hacer frente a los *ataques persistentes avanzados*»

OBJETIVOS DE UN ATAQUE APT

Hemos pasado de los ataques realizados sin un objetivo específico, ataques generalizados, cuyo propósito era causar daño, a los ataques muy avanzados y selectivos (con objetivos claramente definidos). Suelen tener como diana, entre otros, el espionaje empresarial, los objetivos gubernamentales, los activos militares, la

Predicciones de Trend Micro Security 2015

Como hemos apuntado en la introducción, las predicciones en el campo de la ciberseguridad para el año 2015 apuntan a un aumento considerable de los ataques APT.

El informe de Trend Micro (Informe: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-invisible-becomes-visible.pdf) denominado *The invisible becomes visible* (*Lo invisible se vuelve visible*), realiza las siguientes predicciones en el área de la ciberseguridad:

- ✓ Más cibercriminales acudirán a la denominada red oscura (**darknet**[7]) y a foros de acceso exclusivo para compartir y vender productos relacionados con el cibercrimen.
- ✓ Los nuevos métodos de pago móvil introducirán nuevos tipos de ataques.
- ✓ Se verán más intentos de explotar vulnerabilidades en aplicaciones móviles basadas en código abierto (*open source*)
- ✓ Una mayor ciberactividad se traducirá en herramientas e intentos de *hackeo* más grandes y exitosos.
- ✓ Los *kits de explotación* (herramientas que los ciberdelincuentes hacen y venden a terceros para realizar ataques) se dirigirán hacia el sistema Android, en tanto que las vulnerabilidades móviles tendrán un papel importante en la infección de dispositivos.
- ✓ **Los ataques dirigidos (APT) se volverán tan predominantes como el cibercrimen**.
- ✓ La diversidad tecnológica protegerá a los dispositivos de Internet de las cosas contra los ataques masivos, pero no se podrá decir lo mismo de los datos que se procesan.
- ✓ Surgirán amenazas más severas para la banca en línea y para aquellas entidades que tienen una motivación financiera.

DICCIONARIO

[6] **Ataque DoS:** *Denial of Service,* Denegación de servicio, es un tipo de ataque que consiste en dejar fuera de servicio un activo de nuestro sistema de información (recurso o servicio), esto es, que sea inaccesible por las personas o servicios que tengan el derecho de acceso a este. La forma más básica de realizar un ataque de este tipo es inundar a un servidor con peticiones de acceso masivas (servidor de correo electrónico o de páginas Web).

[7] ***Darknet***: es lo que se denomina como *red oscura*, una red privada y distribuida que trata de preservar el anonimato de las personas que intercambian información en ella. Operan aparte de las redes públicas sobre las que se montan, y sus contenidos no son accesible por parte del público en general, además, los motores de búsqueda no suelen buscar en estas redes, con lo que su contenido permanece oculto.

propiedad intelectual, los medios de comunicación masiva y televisión, los operadores de telecomunicaciones y de satélites, las infraestructuras críticas —ver recuadro *Infraestructuras Críticas*—, y la información financiera; es decir, se producen y afectan a todos los sectores y modelos de industrias.

Para realizar ataques APT se suele utilizar una combinación de *malware*[8] específico, en función del objetivo atacado, lo que en la práctica supone que la tarea de detección de este tipo de ataques sea más compleja de lo habitual.

EL ATAQUE PRECURSOR: STUXNET

Stuxnet es un *malware* del tipo APT, quizás es el primer ataque denominado APT; se dio a conocer al público en general en el año 2010, e infectó la central nuclear de Natanz en Irán, que utilizaba centrifugadoras para enriquecer el uranio; **su objetivo era retrasar el programa nuclear iraní** comprometiendo esas centrifugadoras, que si se averiaban hacía que subiera la presión del sistema, que se controlaba a través de válvulas y sensores (APT diseñada para infectar a equipos Windows y sistemas SCADA[9]); por lo tanto, pensando en gobernar los controladores industriales que manejaban esas válvulas y sensores se realizó el ataque, sin llegar al punto máximo, que hubiese consistido en destrozar la central nuclear, teniendo como propósito el «*causar daños frecuentes en la central*», por estrés excesivo. Hubo una segunda fase de ataque en la cual el método de entrada fue a través de la infección de ordenadores de contratistas externos que trabajaban en la central, y que una vez conectados sus equipos a los ordenadores de la central nuclear, infectaran a estos últimos y controlaran los rotores de las centrifugadoras a través de la falsificación de las lecturas de su velocidad de rotación. Esta segunda versión utilizó vulnerabilidades denominadas de *día cero* (*0-day*[10]). Este ataque consiguió pasar desapercibido muchos meses.

FASES DE UN ATAQUE APT

Si bien es cierto que cada ataque APT es diferente en función de cual sea su objetivo, existen unas fases que comparten todos estos ataques, y que son las siguientes:

1. Preparación inicial: estudio y análisis del objetivo y de sus sistemas para detectar posibles debilidades por dónde atacar.
2. Intrusión inicial (aprovechando las debilidades del sistema detectadas): generalmente se realiza a través de la Web (*exploit* remoto) o de archivos adjuntos o hipervínculos asociados a un mensaje de correo electrónico.
3. Instalación del *malware*: una vez dentro de la víctima, se ejecuta el código con *malware*.
4. Conexión de salida: normalmente a través de una herramienta de administración remota (un canal cifrado SSL entre la máquina infectada y un **servidor denominado de comando y control** que manejan las personas autoras del ataque).
5. Expansión: es el punto en el que, a través del dispositivo del usuario final que se ha vulnerado, la APT se propaga lateralmente buscando su objetivo (ordenadores de los administradores del sistema, bases de datos, servidores…)
6. Búsqueda y evasión de datos: se buscan los datos y se transfieren estos sin levantar sospechas de tráfico inusual (por ejemplo, en bloques comprimidos y con contraseña); también se debe conseguir que el ordenador que recibe los datos pase desapercibido.
7. Eliminación de pistas: a través de otros ataques de *malware* (para despistar), y borrado y desinstalación del *malware* que se instaló.

DETECCIÓN DE UN ATAQUE APT

Como ya se ha comentado, las formas tradicionales de defensa no sirven para hacer frente a los

DICCIONARIO

[8] ***Malware***: software malicioso, cuyo objetivo es dañar o infiltrarse en un sistema de información.

[9] **SCADA:** *Supervisory Control And Data Acquisition*, sistemas para la adquisición, control y supervisión de datos de procesos industriales.

[10] ***0-day***: tipo de ataque que consiste en la ejecución de código malicioso que explota vulnerabilidades que son desconocidas por el público en general y también por los fabricantes del producto o servicio.

ataques APT.

Por ejemplo, las técnicas basadas en firmas, como se ha dicho anteriormente, al ser sistemas de protección estáticos (que sólo permiten identificar las ataques ya conocidos), no funcionan en lo que respecta a los ataque APT, que se basan en ser ataques dinámicos y polimórficos (tienen la capacidad de cambiar en el tiempo en función de ciertas variables).

Las soluciones denominadas *sandboxes*[11] basadas en archivos tampoco solucionan el problema, ya que estas soluciones aíslan los procesos en un entorno virtual que analiza los archivos (.EXE, .PDF, ficheros Office de Microsoft, etc.), pero se dejan en el tintero la mayoría de los objetos a analizar, no tienen en cuenta las distintas etapas de los ataques APT, y no establecen correlaciones.

Las medidas de *antimalware* en la nube exigen que los datos sean reenviados a la nube para realizar su análisis, cosa que no suele ocurrir.

Por todo ello, las soluciones de defensa actuales para combatir los ataques denominados APT, complementadas con las soluciones tradicionales, realizan las siguientes acciones:

- ✓ Análisis dinámico y en tiempo real desde diferentes puntos de vista: del tráfico web, del tráfico de correo, de los archivos de la empresa, del tráfico móvil, de los puestos de la empresa o cualquier otro objeto.
- ✓ Una vez realizados estos análisis, los equipos de defensa se interrelacionan cambiándose la información obtenida y estableciendo correlaciones entre esta información.
- ✓ Ejecución, en tiempo real, de los flujos sospechosos en un entorno virtualizado con el objetivo de detectar y bloquear los intentos de extracción de datos. ❑

DICCIONARIO

[11] ***Sandbox***: es una palabra inglesa que significa *caja de arena*, es un **sistema de aislamiento** de procesos usado en entornos de seguridad informática: procedimiento para ejecutar procesos informáticos de manera segura y separada.

[12] **Vulnerabilidades SCADA:** conjunto de guías de interés para la seguridad de los sistemas de control industrial. http://www.cnpic.es/Ciberseguridad/4_Guias_Scada/index.html

Infraestructuras Críticas

Se llama Infraestructuras Críticas (IC) al conjunto de recursos, servicios, tecnologías de la información y redes que proporcionan servicios esenciales, y que, en el caso de sufrir cualquier interrupción no deseada (por causas naturales, técnicas o ataques intencionados), tendría graves consecuencias en los flujos de suministro vitales, en el funcionamiento de los servicios esenciales y en la seguridad. Hay una **Ley 8/2011, de 28 de abril,** por la que se establecen medidas para la protección de las infraestructuras críticas.

Los criterios para determinar la criticidad de una infraestructura son tres: el número potencial de víctimas, el impacto económico y el impacto público.

La citada Ley tiene como objetivos primordiales los siguientes: establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas, en materia de protección de Infraestructuras Críticas, previa identificación y designación de las mismas, impulsando, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo. También se regula a través de esta Ley las obligaciones que deben asumir tanto las Administraciones Públicas como los operadores privados de aquellas infraestructuras que se determinen como *Críticas*.

Las IC, según el **Plan Nacional de Protección de Infraestructuras Críticas,** se pueden dividir en 12 sectores estratégicos: centrales y redes de energía, tecnologías de la información y las comunicaciones, sistema financiero y tributario, sector sanitario, espacio, instalaciones de investigación, alimentación, agua, transportes, industria nuclear, industria química y administración.

El **Centro Criptológico Nacional (CCN)** apoya al Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) en el tratamiento de los ciberataques sobre infraestructuras críticas, y en la actualización de información sobre vulnerabilidades SCADA[12] e incidentes de seguridad informáticos, relacionados con infraestructuras críticas.

CCN Centro Criptológico Nacional

www.ccn.cni.es

ALBOAN:

Estandarización de las encuestas electrónicas

«El Eustat ha creado un *framework* para el desarrollo de los cuestionarios web»

Hasta el año 2008, las aplicaciones web desarrolladas por el EUSTAT para la recogida de datos se diseñaban de forma independiente unas de otras, lo que suponía, en muchos casos, problemas graves en cuanto a la uniformidad de criterios en el diseño, duplicación de código, etc. De hecho, se comprobó que, desde el punto de vista **funcional**, cada una de las aplicaciones desarrolladas cubría todos los aspectos requeridos en el proceso de encuestación, pero, desde el punto de vista de **diseño y construcción**, cada aplicación tenía sus propias características que dependían de las diferentes empresas que las habían desarrollado.

Para evitar estos problemas se puso en marcha un proyecto que tenía estos **objetivos**:

- Remodelar todas las aplicaciones web actuales utilizando una misma plataforma de desarrollo
- Unificar el aspecto visual de todas las aplicaciones web, incluyendo las pautas de diseño (imágenes, tipografía, navegación...), aspectos técnicos (peso, velocidad de carga, accesibilidad...) y de estructura (contenido...)
- Definir un **punto único de entrada** para todas las encuestas web
- Establecer una arquitectura técnica única para simplificar la implantación y el mantenimiento

PLANIFICACIÓN DEL PROYECTO

El proyecto tenía el siguiente plan de trabajo:

- ✓ Crear el portal de entrada único a todas las encuestas web, y se definió también diferentes niveles de autentificación y gestión de perfiles
- ✓ Crear el marco básico de todas las páginas que componen una encuesta web. Para ello, se estableció la organización y jerarquía de las páginas, hojas de estilo comunes para todas las encuestas, mapa básico de navegación y menús, sistema único para la interacción de mensajes de *feedback*, validación y avisos, etc.
- ✓ Crear un repositorio de componentes software comunes a todas las aplicaciones web para reducir el tiempo de desarrollo de las mismas
- ✓ Desarrollar el libro de estilo
- ✓ Crear un único marco de gestión y control de errores a utilizar en todas las aplicaciones web
- ✓ Crear un sistema único de validación de las encuestas web.
- ✓ Homogeneizar los diferentes tipos de ayuda y su visualización

Para llevar a cabo todo este trabajo se estableció una planificación que abarcaba varios años:

- ➢ **2009-2010**: se definió la parte técnica del proyecto, del diseño y del estilo de las futuras encuestas
- ➢ **2011-2012**: se desarrollaron los diferentes componentes software y se adaptó una encuesta piloto al nuevo estándar
- ➢ **2012-2014**: se migraron todas las encuestas web existentes al nuevo *framework* (conjunto de módulos de software que sirven para organizar y desarrollar programas/software). Los nuevos cuestionarios se desarrollan ya directamente con la nueva plataforma

DESCRIPCIÓN FUNCIONAL

Para dar respuesta a las necesidades planteadas, el Eustat ha creado, por tanto, un *framework* para desarrollar los cuestionarios web que son necesarios para las distintas operaciones estadísticas que realiza este Organismo Autónomo.
A la hora de crear este *framework*, el cual facilita los desarrollos y asegura la calidad del resultado final, el Eustat ha buscado cumplir dos objetivos:

1. Mejorar la **usabilidad** de los cuestionarios de forma que faciliten la tarea de los usuarios. (cuestionarios más atractivos, navegación fluida, ayudas adecuadas, etc.)
2. Desarrollar los nuevos cuestionarios web con la suficiente **calidad** y con menos esfuerzo

Diseño general de los cuestionarios

Para llevar a cabo el **libro de estilo** donde se definen todas las normas de diseño de los cuestionarios se hizo un estudio de las recomendaciones realizadas por expertos en la materia, y se definieron, entre otras, estas pautas:

- Usar un esquema por secciones idéntico en todas las páginas del cuestionario, teniendo cada sección una funcionalidad concreta
- Usar el diseño por «Paginación», evitando los deslizamientos tanto horizontales como verticales
- Usar los elementos básicos (*radio buttons*, listas desplegables...) en base al tipo de las preguntas y seleccionando el elemento que mejor se ajuste a ellas
- Diseño específico de las tablas de datos para una mejor compresión de este tipo de información
- Sistemas de ayudas definidos en diferentes niveles

Sistemas de verificación de la información

Con el objeto de evitar al máximo los datos erróneos en las respuestas, se ha diseñado un sistema de validación y control de errores. De hecho, se han definido tres tipos de validaciones:

1. De página: validaciones de controles o entre controles de la misma página
2. De cohesión: validación entre controles de páginas diferentes
3. Longitudinales: validaciones a modo de advertencia sobre controles específicos.

Asimismo, se ha cuidado la forma de presentar los mensajes que se visualizan (intentando que sean lo más *amigables* posible) para aumentar la comprensión del cuestionario.

Navegación

Se ha definido una lógica de navegación que permite el cambio de páginas mediante botones de avance secuencial o mediante un *mapa de navegación*. Este sistema integra el almacenamiento de información de control del cuestionario como puede ser la duración, la fecha de cumplimentación, etc.

Por último, el sistema de navegación incluye un mecanismo de control de grafo que se encarga de activar y desactivar preguntas (o bloques de preguntas) en base a las respuestas dadas en alguna de ellas.

Seguridad de los datos

Respecto a los datos, se ha diseñado un *precuestionario* como punto de entrada único para todos los cuestionarios electrónicos, el cual incluye diferentes medidas de seguridad de **protección de datos**, por una parte, y de **control de accesos**, por otra, así como el registro de otras informaciones de interés que permiten analizar la carga de trabajo a la hora de cumplimentar las encuestas por parte de los usuarios finales.

NUEVOS RETOS

A través de la implantación de este proyecto, el Eustat no sólo ha conseguido los objetivos de **estandarización** de todos los cuestionarios web tanto desde el punto de vista del diseño como de la arquitectura, sino que también ha conseguido **reducir los costes** de desarrollo y de mantenimiento del software de los cuestionarios, así como mejorar la **calidad** de los mismos.

De todas formas, y de cara al futuro, se están abordando ya otros temas como son:

- Definir y construir un «Portal» del encuestado que permita aumentar la interacción del Eustat con los informantes
- Incluir nuevos sistemas de acceso que garanticen la «identificación» y autenticación de las personas encuestadas
- Crear versiones *app* para dispositivos móviles
- Ampliar el *framework* con nuevos componentes para incluir nuevas funcionalidades
- Y, por último, incluir sistemas que permitan evaluar la satisfacción de los usuarios al finalizar las encuestas. ❑

«Gracias a este proyecto, el Eustat ha conseguido reducir los costes de desarrollo y de mantenimiento de todas las encuestas web, así como mejorar la calidad de las misma»

[+info]:

Web del Eustat:

http://www.eustat.eus

ALBOAN

¡¡BREVES!!

nº 51

Marzo de 2015

Telefonía móvil: «modo avión»

En los aviones no se podía viajar con dispositivos electrónicos portables (PED, *Portable Electronic Devices)* conectados (por ejemplo, teléfonos inteligentes, tabletas, ordenadores portátiles, e-readers o reproductores MP3), hasta que la EASA (*European Aviation Safety Agency,* la Autoridad Europea de la Seguridad Aérea) autorizó, en el año 2013, el uso de estos PED, **siempre y cuando estos se configurasen en «modo avión»** (*aeroplane mode*), es decir, que no estuviesen transmitiendo: se desactivan las conexiones inalámbricas del dispositivo, y, de este modo, se evita el envío y recepción de señales de radio (Wi-Fi, Bluetooth, 3G…), también se desactivan las conexiones de datos y las de voz.

La EASA había estado trabajando con el objetivo de que las aerolíneas permitiesen el uso de estos dispositivos en sus vuelos con libertad, al igual que ocurre con otras clases de transporte, como, por ejemplo, el transporte ferroviario. Por todo ello, desde el 26 de septiembre de 2014, consiguió que se permitiesen su uso, independientemente de si el dispositivo está transmitiendo o no. Por supuesto que, en última instancia, le corresponde a cada línea aérea permitir o no el uso de los PED transmitiendo (cada línea debe asegurar que los vuelos no se ven afectados por la transmisión de este tipo de señales).

Por razones de seguridad la EASA regula ciertas condiciones para la utilización de los PED en las aeronaves operadas por las compañías aéreas europeas, y destaca que estas compañías pueden ser más restrictivas que la propia EASA.

Web EASA: http://www.easa.europa.eu/

Primeros móviles con Ubuntu

La empresa de software Canonical y la compañía BQ acaban de presentar en Londres el Aquaris E4.5 Ubuntu Edition, el primer *smartphone* con Ubuntu que saldrá al mercado. (Ubuntu es hoy en día una de las distribuciones de **Linux** más populares que existen en el mundo).

Según los expertos, se trata de un terminal de gama media dirigido principalmente a los llamados *early adopters*, es decir, a personas entusiastas de probar nuevos productos.

Según ha informado la empresa BQ, el nuevo dispositivo será «libre», pudiendo de esta forma ser usado con cualquier operador de telefonía.

Las principales características técnicas del Aquaris E4.5 Ubuntu son las siguientes:

Pantalla de 4,5 pulgadas (resolución de 960×540 píxeles), cámara frontal de 5 megapíxeles y trasera de 8, procesador SoC Mediatek Quad Core ARM Cortex A7 a 1.3 GHz, 1GB de memoria RAM y 8 GB de almacenamiento interno, batería de 2.150 mAh, tarjeta MicroSD, posibilidad de usar dos tarjetas SIM (Dual SIM). Sus medidas son 9 mm. de grosor y 123 gr. de peso.

Otra de sus principales características que tiene el dispositivo es la navegación que ofrece mediante las vistas denominadas *Scopes* [modo de acceso a los servicios más utilizados del teléfono desde la pantalla principal, los cuales son agrupados por temáticas como «música», «eventos», etc., siendo su equivalente las *apps* que se utilizan habitualmente en los teléfonos móviles).

En referencia a las futuras actualizaciones de software (sistema operativo y aplicaciones) se encargará Canonical.