EUSKO JAURLARITZA
GOBIERNO VASCO

Aurrera!

Nº 39
septiembre de 2010

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

Una vez finalizadas las vacaciones de verano retomamos la tarea de daros a conocer aquellos temas sobre nuevas tecnologías que se producen a nuestro alrededor. En esta ocasión, con el primer artículo, y tomando como punto de partida el sistema operativo Debian, queremos dar respuesta a algunas de las preguntas que muchas personas se hacen sobre el mundo del software libre y las múltiples distribuciones que existen hoy en día: ¿Por qué existen tantas distribuciones de Software Libre? ¿Es bueno que haya tantas? ¿Cómo se gestionan? ¿Qué son y quiénes integran las llamadas "comunidades"? ¿Qué función tienen?

En el segundo tema, titulado "Sistemas de Alerta Temprana", profundizaremos en ese concepto para explicaros todo lo que abarca e incluye, ya que, si bien se trata de un servicio de "vigilancia" y prevención que como tal no es nuevo, si continúa siendo bastante desconocido para muchos de nosotros.

Como consecuencia de la reciente adjudicación del servicio de telecomunicaciones del Gobierno Vasco para el periodo 2010-2013, el cual permitirá, entre otras cosas, dotar de los servicios de telefonía móvil al personal de la Red Corporativa que así lo requiera, damos un rápido repaso a los nuevos equipos que están ya disponibles, aspectos a tener en cuenta para su correcta gestión, así como una serie de recomendaciones de "buenas prácticas" para hacer un buen uso de los mismos.

Dentro del apartado "Breves", en esta ocasión os explicamos, en primer lugar, qué son los barnetegis tecnológicos y que nos pueden ofrecer y, en segundo lugar, os detallamos la información que esconden las fotos que hacemos.

Antes de acabar, desde la Dirección de Informática y Telecomunicaciones (DIT), y dado que dentro de unos días nuestro Boletín Aurrera cumple 10 años, queremos agradecer a todas las personas que han hecho posible este proyecto, el seguimiento e interés que habéis mostrado hacia el Boletín Aurrera, así como la aportación de los colaboradores que hemos tenido durante esta última década.

Gracias!!

El mundo de Debian

Aprovechando que recientemente se ha celebrado el encuentro mundial de desarrolladores de Debian, llamado DebConf, a lo largo de este artículo repasamos las principales características de este sistema operativo y todo lo que le rodea: distribuciones existentes, formas de gestionarlas, etc.

DICCIONARIO

[1] **Núcleo o Kernel:** software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora, es decir, se encarga de decidir qué programa podrá hacer uso de un dispositivo hardware y durante cuánto tiempo.

[2] **GNU:** http://es.wikipedia.org/wiki/GNU

[3] **Distribuciones:** relación completa de distribuciones existentes

http://distrowatch.com/stats.php?section=popularity

Del 1 al 7 de agosto pasado se ha celebrado en la Universidad de Columbia (Nueva York) la conferencia DebConf10, encuentro mundial de la comunidad de desarrolladores de Debian. En esta ocasión algunos de los temas de interés tratados a lo largo de casi un centenar de charlas han sido *cloud computing*, virtualización, proyectos Debian para el *Google Summer of Code*, colaboración entre Ubuntu y Debian, procesos de calidad en el software de Debian, despliegue de infraestructuras masivas, software científico, *Open Street Map*, etc.

Por todo ello, se recoge aquí una exposición de esta interesante distribución GNU/Linux y todo lo que la rodea.

DISTRIBUCIONES GNU/LINUX

Los sistemas operativos Windows, Mac OS, Unix, GNU/Linux, Minix, etc. están formados por un núcleo o kernel[1], como son Linux, BSD o Hurd, y una serie de programas (ej. GNU[2]) alrededor de dicho núcleo. El sistema operativo GNU/Linux data del año 1992, y una de las particularidades del mismo es que debido a que las licencias de sus componentes permiten redistribuirlos de forma libre, no existe un único GNU/Linux sino que han evolucionado distintas familias del mismo denominadas "*distribuciones*" o "*distros*", que no son sino agrupaciones o conjuntos empaquetados de los componentes del sistema operativo junto con otros programas extra (ej. ofimática, multimedia, bases de datos, y un larguísimo etcétera), todo ello bajo una marca o nombre distintivo como pueden ser Ubuntu o Debian.

De hecho, a día de hoy existen más de **300 distribuciones**[3]. Pero, ¿por qué se da esta gran diversidad? Los factores que diferencian a unas de otras son variados.

En primer lugar está la titularidad o quién se encuentra detrás de cada distribución, si una empresa o una comunidad de personas desarrolladoras.

Un segundo aspecto es el producto o contenido software de cada distribución, que a su vez puede desglosarse en:

- **Orientación y Funcionalidades**, esto es, en qué se focaliza cada distribución: las hay generalistas y las hay de propósito específico para seguridad, multimedia,... Todas las del segundo grupo, las multimedia, incluyen programas de su área, de modo que una vez instalada la distribución no hay que andar haciendo instalaciones de software adicional.
- **Modalidades y Versiones de los programas incluidos**. Un caso típico puede ser si la distribución funciona con un entorno gráfico

KDE o Gnome o sólo dispone de consola de texto. Igualmente cabría señalar aquí aspectos más técnicos, como el tipo de paquetes de software, el sistema de ficheros según el cual queda formateado el disco tras la instalación, o las características de seguridad que vienen por defecto.

- **Tamaño de la distribución** en cuanto a la cantidad de programas disponibles o número de paquetes incluido.
- **Licencias de los programas incluidos**: es posible que una distribución incluya programas cuyas licencias no sean del todo libres. Por lo tanto, permiten su empaquetamiento, pero no el acceso al código fuente o la modificación del mismo. A modo de ejemplo, una distribución podría incluir un paquete con el instalador del *plugin* de Flash, que es un software privativo propiedad de Adobe, gratis pero no libre. También entraría aquí el caso de programas cuyo uso no se permite en un determinado territorio geográfico, por ejemplo, que existan restricciones según las políticas de exportación de software de criptografía en EE.UU.[3].

- **Requisitos hardware de la plataforma** sobre la que corre, diferenciándose entre arquitecturas, memoria RAM y espacio de disco. Así, puede haber distribuciones para PC orientadas a puesto de escritorio, pero también para servidores, sistemas embebidos como son los *routers* o teléfonos móviles, super-computadores, ordenadores antiguos o con muy pocos recursos,...
- **Localización**[4] **e internacionalización**[5] **(Idiomas)**: unas distribuciones están traducidas a muchos idiomas y otras a menos. En el caso de Ubuntu, la versión más reciente, de abril de 2010, considera que de las 218 lenguas, se dan por traducidas del todo 29, entre ellas el euskera[6]. Además de los idiomas, durante unos años estuvo de moda la tendencia de hacer distribuciones localizadas o personalizadas a ámbitos geográficos, donde se incluían elementos visuales y algún software específico de cada zona. Un ejemplo puede ser LinEx, la "*distro*" promovida por la Junta de Extremadura. Hoy en día esta práctica está en declive por motivos varios.

- **Facilidad de instalación y uso**: aunque algunas distribuciones son muy sencillas de instalar y usar, principalmente porque están orientadas al usuario medio, otras más específicas pueden requerir mayores conocimientos, por ejemplo de supercomputación. Aquí cabe señalar también las alternativas de instalación (desde CD, DVD, USB o por red), y la posibilidad de funcionamiento en modo "*live*", esto es, la capacidad de funcionar arrancando desde CD o *pendrive* USB sin necesidad de instalar nada en el disco duro.

Otra diferenciación entre distribuciones está en el *portfolio* o catálogo de servicios ofrecidos, y el precio y calidad de los mismos. Algunos ejemplos son:

- El **reporte de errores y corrección** de los mismos. Algunas *distros* lo proporcionan gratis mediante paneles web o listas de correo, y no todas las *distros* solucionan errores a igual velocidad.
- La frecuencia de aparición de **nuevas versiones**, y la calidad de las mismas.
- El envío de **soportes físicos** (CD, DVD, USB) para la distribución, de forma adicional o reemplazando a la posibilidad de descarga por Internet.
- La **formación** presencial y el envío de materiales físicos de formación (manuales en papel).

DICCIONARIO

[3] **Software de criptografía**: www.debian.org/legal/cryptoinmain

[4] **Localización:** operación por la que sobre un conjunto de programas que ya han sido previamente internacionalizados se les proporciona toda la información necesaria para que pueda manejar su entrada y su salida de un modo que sea correcto respecto a determinados hábitos lingüísticos y culturales, como por ejemplo el símbolo de la moneda o el orden del mes, día y año de las fechas.

[5] **Internacionalización:** operación por la cual se modifica un programa o conjunto de programas para que puedan adecuarse a múltiples idiomas y convenciones culturales.

[6] **Traducciones de Ubuntu:** http://people.ubuntu.com/~dpm/ubuntu-10.04-translation-stats.html

Algunas distribuciones tienen dos ediciones, una gratis y otra de pago en concepto de servicios. Otras distribuciones, sin embargo, tienen una única edición, donde en la mayoría de los casos ésta es gratuita, aunque en algunos casos es de pago.

Todos esos servicios pueden ser proporcionados desde la "*comunidad*", desde la empresa matriz o desde otras empresas intermedias. Podría ser el caso, por ejemplo, de una empresa andaluza que da soporte oficial de Ubuntu[7], cuya empresa madre se llama Canonical y tiene la sede principal en Sudáfrica.

Finalmente, cabría hablar de otros aspectos, como la **antigüedad** de las distribuciones y la **popularidad** de las mismas, en función de la cual será mayor o menor la base de usuarios (algunas de las más populares son Ubuntu, Red Hat, Suse y Debian).

Las diferentes distribuciones no son independientes entre ellas, sino que unas reutilizan trabajo de las otras. Por ejemplo, muchos de los paquetes que hace Debian son incluidos en Ubuntu, o las traducciones de Debian se incluyen en Red Hat.

Fuente: www.linuxjournal.com / Fecha: agosto 2010

Como recapitulación de todos los factores indicados, a pesar de que a primera vista la multiplicidad de *distros* pueda parecer un despilfarro de esfuerzos disgregados, tiene mucho sentido, porque se ofrecen muchas posibilidades de modo que, en cada escenario concreto, se puede elegir la alternativa más adecuada. Dicho de otro modo, no existe un único sistema operativo que sea perfecto para todas las situaciones y puede ser bueno el poder elegir.

Otros fabricantes de sistemas operativos privativos ofrecen múltiples alternativas de un producto que es el mismo en todos los casos, pero que se diferencia en que se restringen parte de las funcionalidades según el precio de cada edición. La explicación a esta oferta es diversificar el valor de venta mediante una estrategia de marketing para tratar de captar más clientes en el mercado.

"Las *distribuciones* son conjuntos empaquetados de los componentes del sistema operativo junto con otros programas extra, todo ello bajo una marca o un nombre distinto."

DEBIAN, UNA DISTRIBUCIÓN Y UNA GRAN COMUNIDAD

Esta distribución nació en agosto de 1993, siendo por ello la más antigua que existe a día de hoy junto con Slackware, y siempre se ha mantenido dentro de las más populares. A partir de Debian, se han creado más de 50 distribuciones derivadas, siendo las más famosas: **Ubuntu** (en sus distintas ediciones), **Knoppix** y **Backtrack**.

Debian es una distribución que se caracteriza por una gran estabilidad y calidad, y está menos orientada al marketing de usuario común frente al caso de, por ejemplo, Ubuntu.

Debian cuenta con el record de arquitecturas soportadas, entre diez y quince según versiones. Esto implica que una misma forma de trabajar con el sistema operativo vale para distintos entornos, por ejemplo, PCs de escritorio, servidores, sistemas embebidos o mainframes. Incluso, en la próxima versión funcionará no sólo con el núcleo Linux (Debian GNU/Linux) sino también con el BSD (Debian GNU/kFreeBSD).

La versión estable de esta distribución cuenta con más de 28.000 **paquetes gratuitos**[8]. La gran mayoría de ellos son libres, pero también hay una sección dentro de Debian denominada *non-free* con algunos paquetes que no lo son.

Curiosamente, toda esta producción ingente de software proviene del trabajo de la "*comunidad*" y no de una empresa como tal. ¿Y quiénes forman la "*comunidad*"? Todas aquellas personas que desde hace 17 años se empeñan en construir un sistema operativo libre: programadores, administradores de sistemas, diseñadores, etc. que bien dedicando su tiempo personal o haciendo contribuciones desde empresas como HP o Google, decidieron aportar

DICCIONARIO

[7] **Ubuntu:** palabra de origen africano (Zulú y Xhosa) que no tiene una traducción exacta. En el fondo es un sentimiento, una forma de vida, una especie de ideología muy arraigada especialmente en Sudáfrica. Se podría resumir en que la existencia propia está íntimamente ligada con la de los demás, y viceversa.

La traducción más utilizada es "ser humanitario con los demás". Aunque la palabra en sí no hace referencia al Sistema operativo Ubuntu Linux, si lo hace a la filosofía que esta detrás de esta distribución, la cuál es sacar a la humanidad de la esclavitud y hacer énfasis en que el conocimiento es de todos.

[8] **Paquetes Debian:** http://packages.debian.org/stable/allpackages

a esta obra de construcción colectiva, y que hoy cuenta con un gran respeto entre el resto de las distribuciones.

Pero lejos de ser una nebulosa de personas sin orden ni concierto, la comunidad está estructurada según 18 grupos de trabajo, y cuenta con múltiples líneas de proyectos y productos[9]. Todo ello bajo un **contrato social**[10] que asegura cuestiones tales como la libertad del software, la no discriminación, etc. y que han de aceptar quienes quieren entrar a contribuir oficialmente en la distribución.

La comunidad mundial de Debian se reúne una vez al año en la **DebConf**, para debatir sobre aspectos tecnológicos, jurídicos y éticos, así como para exponer experiencias de éxito e intercambiar conocimiento de distinta naturaleza.

Todo lo indicado no equivale a decir que no hay soporte profesional de la distribución Debian. Muy al contrario, existen empresas que basan su negocio en la misma. Bien empleando esta distribución como base de su producto/servicio (ej. una empresa de albergue web, o de CMSs, o de telefonía sobre Asterisk), o bien dando soporte a clientes que la utilizan; un caso emblemático es el de la ciudad de Munich[11], que con la migración de sus 14.000 ordenadores de Windows a Debian, ha conseguido traccionar el sector local de software promoviendo, además de la independencia tecnológica, el desarrollo económico de la región.

> "La *comunidad* mundial de desarrolladores de Debian se reúne una vez al año en la «DebConf»."

CONCLUSIONES

En consecuencia, gracias al largo recorrido de esta distribución, a su amplia base de uso, a la fortaleza de su comunidad, y a la gran disposición de software y documentación, están dispuestas las condiciones para poner en marcha infraestructuras soportadas sobre la misma, así como para promover empresas de base tecnológica que presten servicios en torno a la distribución Debian. Y, aquí, en Euskadi, también hay personal altamente cualificado para emprender esta estrategia.

En suma, Debian constituye una alternativa seria a tener en cuenta para cualquier apuesta tecnológica que pretenda conjugar calidad y libertad. ❑

eusLinux

El Gobierno Vasco, desde la Viceconsejería de Política Lingüística (Dpto. de Cultura), ha promovido la traducción-localización al euskera de algunas de las aplicaciones informáticas que engloba el movimiento del software libre, entre ellas, eusLinux, la cual está basada en Debian GNU/Linux.

El objetivo final del Departamento de Cultura ha sido promover la presencia del euskera en el ámbito de las TIC así como desarrollar y poner al alcance de la ciudadanía recursos, herramientas y nuevas aplicaciones en euskera.

Las aplicaciones o utilidades incluidas en esta distribución son, entre otras, las siguientes:

GNome (interface de escritorio), *Gnumeric* (hoja de cálculo), *Balsa* (cliente ligero de correo), *Anjuta*, *Glade* y *Alleyoop* (herramientas para programar aplicaciones), *Brasero* (aplicación para grabar CD/DVDs), *Banshee* (reproductor de música) y varios juegos.

Esta distribución se puede descargar gratuitamente desde la web www.euskara.euskadi.net, en el apartado "*Descarga de software en euskera*".

DICCIONARIO

[9] **Proyectos y Productos de Debian**: http://wiki.debian.org/Teams

[10] **Contrato Social**: www.debian.org/social_contract

[11] **Información sobre la migración de Múnich**: http://wiki.debian.org/PressCoverage2006#MunichswitchestoDebian

SAT: Sistemas de Alerta Temprana

Las Alertas Tempranas existen en muchos campos y áreas de nuestra vida cotidiana, siendo un complemento importante dentro de lo que se conoce como la gestión de riesgos. En este artículo vamos a hablar de los Sistemas de Alerta Temprana dentro del sector de las Tecnologías de la Información y las Comunicaciones (TIC).

DICCIONARIO

[12] **ISO 27002:2005:** estándar internacional certificable centrado en reducir el riesgo al que están expuestos los activos de información. Son un conjunto de controles que comprenden las mejores prácticas en seguridad, y es el resultado de la estandarización de la primera parte del BS7799.

(Ver boletín AURRERA nº 33, artículo "*Seguridad en dispositivos móviles externos*")

En cualquier organización, para gestionar el riesgo, como es lógico, primero se debe valorar. El trabajo de realizar un **análisis y gestión de riesgos**, es, por un lado, laborioso, y, por otro lado, costoso. Dentro de esta área de la gestión de riesgos, y con la finalidad de anticiparse a los incidentes y anomalías, se crean los **Sistemas de Alerta Temprana (SAT)**.

ANALIZAR Y GESTIONAR EL RIESGO

Análisis del riesgo

La evaluación de la exposición al riesgo comienza con una **identificación de los activos** de información (mapa de activos), después, como se ha comentado al principio, **se valoran** (se debe conseguir una uniformidad de criterio de todas las personas que intervienen en estas valoraciones), esta fase es muy importante, ya que se debe relativizar el riesgo, centrándose en lo más importante. Posteriormente **se identifican las amenazas** para cada activo, así como la probabilidad de que esta amenaza se materialice (al resultado, generalmente negativo, de la materialización de una amenaza se le conoce como «impacto»). También se identifican las **vulnerabilidades**, y la posibilidad de que estas sean explotadas por las amenazas, así como la exposición al riesgo de los activos; con todo ello se priorizan las amenazas según la exposición que éstas tengan al riesgo. En este punto se puede realizar una evaluación del riesgo, usando una serie de criterios, como son: el impacto económico que produciría ese riesgo, el tiempo de recuperación de la organización una vez ocurrido, la posibilidad de que dicho riesgo ocurra y la posibilidad de interrumpir actividades de la empresa.

> **"Postura de seguridad: conjunto de iniciativas, procesos y actividades de seguridad que se llevan a cabo en la Organización con el fin de alcanzar los objetivos de seguridad planificados."**

Gestión del riesgo

Un buen análisis y gestión de riesgos va a permitir a la organización tomar decisiones para establecer una política de gasto correcta y justificada, ya que es en este punto donde se debe minimizar el riesgo, a través de una serie de opciones: **reducirlo**, **aceptarlo** (cuando, por ejemplo, la probabilidad es ínfima o el coste que supone evitar ese riesgo es mayor que el coste del activo a proteger), **transferirlo** (es el caso, por ejemplo, en el que se contrata un seguro) o **evitarlo**.

En definitiva lo que se está realizando es una política centrada en reducir el riesgo al que están sujetos los activos de información.

El estándar para implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) es el modelo ISO 27002:2005[12].

QUÉ ES UN SAT

Un Sistema de Alerta Temprana (SAT) no es sino un dispositivo complejo que avisa con antelación de la posibilidad de un hecho que puede causar un desastre, con el único fin de evitar que este ocurra. Los SAT se aplican tanto para anticiparse a los eventos naturales (terremotos, inundaciones ...), a los de origen humano (por ejemplo, conflictos de guerra), como al área de las TIC (la que nos ocupa en este artículo), siempre y cuando estos eventos puedan desembocar en desastre.

AMENAZAS

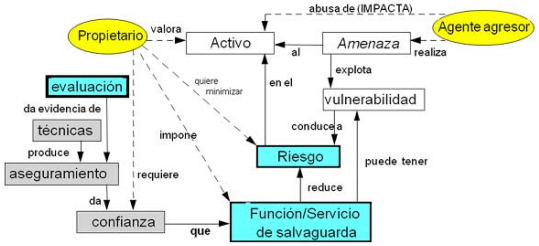
El Manual de seguridad PLATEA define el

concepto de **amenaza** del siguiente modo: «*cualquier circunstancia o evento capaz de causar daño a un sistema en la forma de denegación de servicio o destrucción, revelación no autorizada o modificación de datos*».

Los ataques dirigidos a través de código dañino (*malware*) , tales como **troyanos**[13], **ataques de día cero**[14] o **Botnets**[15] son cada día más peligrosos y menos visibles, y el objetivo no es otro que el de generar beneficios a su autor, bien de forma directa (por ejemplo, troyanos bancarios, que actualmente se distinguen por tener un código dañino muy evolucionado, como puede ser la captura de formularios web, lo que se conoce como *form grabbing,* o la técnica de robo de certificados) o de forma indirecta (como puede ser la distribución de correo basura).

Algunas formas actuales de malware son las siguientes:

- **Ingeniería social**[16], como medio para infectar sistemas sigue teniendo bastante vigencia
- **Distribución de software antivirus dañino** (se presentan como un antivirus legítimo alertando al usuario de que su sistema está infectado, un ejemplo es el *Antivirus Agent Pro*)
- **Toolkits de exploits**, que son vendidos en el mercado negro (son paquetes de código HTML



y JavaScript que los delincuentes diseñan para explotar vulnerabilidades de los navegadores de los usuarios)

- **Troyanos backdoor**, o puertas traseras, suelen comprometer objetivos muy específicos con el objeto de conseguir información sensible
- **Técnicas de rootkit** (ver recuadro "*Fases de una intrusión*"), que estrictamente no se pueden considerar malware, pues son utilizadas por el malware para ocultar su presencia en un sistema, prolongando el tiempo de infección en el sistema atacado
- **Modificadores de DNS** (*Domain Name System*, asocian nombres de dominios en Internet a direcciones IP)
- **Software malicioso que podemos encontrar en las redes sociales**, que aprovechan la confianza de los usuarios en estos mecanismos de comunicación, como, por ejemplo, el gusano *Koobface*, que instala programas antivirus dañinos. Ya existe la primera generación de software anti-spam y anti-malware para redes sociales
- **Botnets DOS** (*Denial of Service*, Denegación de Servicio), tienen un impacto bajo sobre los usuarios infectados, ya que los atacantes usan estos sistemas infectados para atacar a otras entidades, si bien, el usuario infectado pierde ancho de banda y algunos recursos del sistema.

ACTUAR ANTES DE QUE SE PRODUZCA UN INCIDENTE

Actuar contra las amenazas

El objetivo principal de los SAT es tanto la **protección proactiva**, es decir, aplicar medidas antes de que se produzca un incidente o que éste sea detectado, como la **protección reactiva**, una rápida detección que posibilita aplicar medidas de contención que eliminen la amenaza, y, de este modo, eviten o reduzcan el incidente, tanto en su impacto como en su alcance.

Estas medidas pueden combinarse con los procesos de monitorización que ya se dispongan dentro del sistema corporativo.

Como curiosidad, cabe destacar que las medidas

FASES DE UNA INTRUSIÓN

- **Fase de vigilancia**

El atacante intenta aprender todo lo posible sobre el sistema que quiere atacar.

- **Fase de explotación del servicio**

Describe la actividad que permitirá al atacante hacerse con privilegios de administrador en función de la fase anterior.

- **Fase de ocultación de huellas**

Realiza las actividades que le permiten pasar desapercibido ante el sistema, tales como eliminación de entradas sospechosas en ficheros de registro, instalación y modificación de comandos ...

- **Fase de extracción de la información**

El atacante extrae la información que le resulta de interés.

DICCIONARIO

[13] **Troyano:** el nombre proviene de la historia del caballo de Troya que menciona Homero en su libro "*La Odisea*", no es sino un software malicioso que se presenta al usuario como un software legítimo e inofensivo, pero que al ejecutarlo causa daños.

[14] **Ataques de día cero:** *zero-day* ó *0 day*, es una amenaza informática que aprovecha vulnerabilidades de sistema o aplicaciones que no disponen de una solución o parche conocido.

[15] **Botnet:** es un programa informático que permite a un atacante tomar el control de un equipo infectado, al que se le conoce como "*zombie*".

[16] **Ingeniería Social:** comprende todas las tretas, engaños y demás técnicas (no tienen que ser informáticas) para sacar información confidencial a los usuarios (ver boletín AURRERA nº 13, artículo "Ingeniería Social")

Para más información, tenéis el artículo "*Seguridad: Virus*" del AURRERA nº 3)

de tipo proactivo son las que están implantando muchas empresas de software antivirus: realizan una monitorización y análisis de la conducta de todos los programas instalados y en función de cuál sea esta conducta toman decisiones, lo cual no deja de ser sino un Sistema de Alerta Temprana.

SISTEMAS DE DETECCIÓN DE INTRUSOS

Conocidos también con los nombres de Sondas, generadores de eventos, sensores o IDS[17]

Son infraestructuras complejas que permiten, a través de reglas heurísticas, detectar cuando es atacado un sistema informático, entendiendo "ataque" como la utilización del mismo de una forma no autorizada. Estas detecciones son almacenadas como registros de información (*logs*), que después de ser estudiados a través de **técnicas de análisis forense**, puede apreciarse qué es lo que realmente ha sucedido dentro del sistema informático.

Los Sistemas de Alerta Temprana utilizan estas infraestructuras para realizar su labor.

Estos sistemas de detección, debido a su complejidad, deben evitar lo que se llama "falsos positivos", ya que, si los porcentajes de falsos positivos son muy altos, inhabilitan el resto de información registrada, y el sistema queda sin validez.

Desde hace un tiempo se intenta estructurar y unificar la arquitectura de los IDS, existiendo una definición de la misma realizada por el *Common Intrusion Detection Framework*, que identifica cuatro componentes:

- ✓ Generador de eventos
- ✓ Motor de análisis
- ✓ Utilidades de almacenaje
- ✓ Unidades de respuesta

La taxonomía de los generadores de eventos varía según la función de los mismos:

- En función del enfoque
  - Detección de anomalías (se basa en la creación de perfiles de uso durante un determinado período de tiempo)
  - Detección de usos incorrectos (es el más utilizado, se basa en el conocimiento específico de determinados ataques)
- En función del origen de datos
  - Detección de Host local (HIDS, amenazas a nivel de Host local)
  - Detección de red (NIDS, reciben datos de la red local donde están instalados)
  - Híbridos (sensores en cada Host y en cada segmento de red)
- En función de su estructura
  - Distribuidos (los sensores se comunican entre sí)
  - Centralizados (los sensores transmiten información a un sistema central)
- En función de su comportamiento
  - Pasivos (no realizan acciones, sólo envían alertas)
  - Activos (realizan acciones por su cuenta, lo cual puede ser peligroso en algún caso)

De cualquier modo tenemos que ser conscientes de que la detección de intrusos es un problema de difícil solución, debido a la naturaleza impredecible del ser humano, si bien muchas veces las pautas de actuación de los atacantes son muy similares. En definitiva, son sistemas complejos que requieren un mantenimiento, con el objetivo de minimizar los falsos positivos.

SAT en la Red Corporativa del Gobierno Vasco

En la Red Corporativa Administrativa del Gobierno Vasco (RCAGV) hay instalados **sensores de detección y prevención de intrusos (IDP**[18]**)** monitorizando el tráfico en el perímetro de acceso a Internet y en el propio Datacenter. Estos sistemas son capaces de detectar y bloquear ataques previamente configurados (DoS, Fuerza bruta, Gusanos...), enviar alertas vía correo electrónico y realizar informes personalizados.

COMUNICACIÓN TECNIMAP 2010: CCN-CERT SAT

En el pasado **Tecnimap**[19] **2010** que se celebró en Zaragoza, una de las comunicaciones fue la denominada "**CCN-CERT Sistemas de Alerta Temprana**", adscrita a la línea de trabajo «*Iniciativas legales y tecnológicas. Seguridad, conservación y normalización de la información, formatos y aplicaciones*».

El Sistema de Alerta Temprana expuesto cuenta con dos vías: por un lado, la **monitorización de la Red SARA** (Red de intercomunicación de todos los organismos de la Administración Pública Española), y por otro, la **monitorización del tráfico perimetral de los accesos a Internet** de las

DICCIONARIO

[17] **IDS:** del inglés *Intrusion Detection System*, sistema de detección de intrusos. Una intrusión es una secuencia de acciones realizadas por un usuario o proceso deshonesto, con el objetivo final de provocar un acceso no autorizado sobre un equipo o sistema.

[18] **IDP:** del inglés *Intrusion Detection and Prevention, trabaja como* los sistemas IDS, además tiene un carácter preventivo.

[19] **Tecnimap:** es un encuentro que reúne a representantes del ámbito de las tecnologías de la información y las telecomunicaciones de las distintas Administraciones Públicas, las principales empresas del sector y a muy diversos expertos relacionados con este campo. Se trata de un importante espacio de intercambio de experiencias, ideas y proyectos en materia de tecnologías de la información y servicios públicos.

www.tecnimap.es

distintas administraciones, a través del despliegue de sondas individuales, en las salidas de Internet, lo que se conoce como **IDS**.

A través de estas dos vías el **Centro Criptológico Nacional (CCN)** puede detectar todo tipo de ataques, evitando que se expandan, respondiendo a estos ataques de forma rápida, a la vez que se pueden generar **normas de actuación** para evitar futuros ataques.

CCN-CERT: SAT DE LA RED SARA

El sistema se basa en la correlación de registros de datos (*logs*) sobre las áreas de conexión de la Red SARA, mediante la utilización de sensores, permitiendo detectar de manera proactiva las anomalías y ataques del tráfico que circula entre los organismos conectados a dicha Red, dejando claro que el tráfico dentro de la red del Organismo no es cuestión de este SAT. Las incidencias son catalogadas por el sistema, que son elevadas a incidencias de seguridad en función de la evaluación que se realiza de ellas, mediante el trabajo de un equipo de expertos en seguridad.

CCN-CERT: SAT DE INTERNET

A través de un convenio con el CCN-CERT se coloca una sonda individual para controlar la red perimetral de acceso a Internet del Organismo que realiza el convenio; esta sonda se encarga de recolectar la información de seguridad detectada y clasificada como importante, la misma es filtrada, y, posteriormente, se envían los eventos de seguridad hacia el sistema central (hacia el sistema central de sondas, que reside en el CCN), para que éste realice una correlación entre los distintos elementos y los diferentes dominios. La principal ventaja es que la sonda puede ser gestionada por el Organismo, actualizándola e incluyendo nuevas fuentes, así como refinando las reglas que permiten la detección de eventos. Estos eventos son transportados desde el Organismo hacia el sistema central por canales seguros (VPN, SSL...) ❑

RED SARA

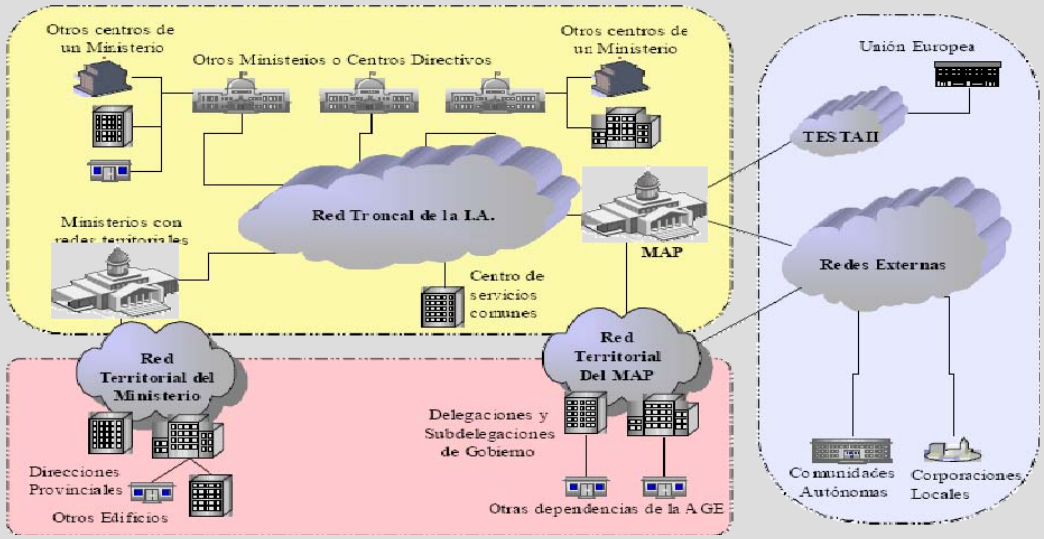
La **Red SARA** permite la interconexión de las administraciones públicas, facilitando el intercambio de información y servicios entre ellas.

A través de la **Red SARA** los Ministerios, las Comunidades Autónomas, los Entes Locales y otros organismos públicos pueden interconectar sus redes de una manera fiable, segura, capaz y flexible.

Además, a través del enlace de la Red SARA con la **red transeuropea sTESTA**[20] las Administraciones Públicas españolas se pueden interconectar con redes de instituciones europeas y de administraciones de otros Estados miembros de la UE, para el despliegue y acceso a los servicios paneuropeos de administración electrónica.

El Plan de direccionamiento e interconexión de redes en la Administración facilita la interconexión de las redes de las Administraciones Públicas a través de la Red SARA.

Fuente: http://www.csae.map.es/



DICCIONARIO

[20] **sTESTA:** *Secure-TESTA*, red IP aislada de Internet que interconecta las redes administrativas de los Estados miembros y de las Instituciones y Agencias Europeas.

Fuente: www.csae.map.es/csi/idabc/capitulo5.htm

ALBOAN:

Telefonía y buenas prácticas

Servicio de Red Corporativa Administrativa

"Las Direcciones de Servicios serán las responsables de controlar y centralizar las peticiones de sus usuarios."

Recientemente, el Gobierno Vasco, a través del Servicio de Red Corporativa Administrativa (perteneciente a la Dirección de Informática y Telecomunicaciones —DIT—), ha resuelto el expediente KM/2010/045. Dicho expediente, denominado "*Servicios de telecomunicaciones a la Administración de la Comunidad Autónoma del País Vasco 2010-2013*", va a permitir al personal de la Red Corporativa Administrativa del Gobierno Vasco (RCAGV) disponer, entre otros aspectos, de los últimos modelos de teléfonos móviles, así como de nuevas funcionalidades en el servicio de telefonía.

Como consecuencia de ello, tanto los técnicos como los altos cargos del Gobierno disponen desde hace varias semanas de los terminales proporcionados por la empresa adjudicataria, en este caso, la UTE Telefónica de España S.A.U. y Telefónica Móviles España S.A.

Mediante este artículo pretendemos exponer aquellas mejoras que van a obtener los usuarios finales gracias, principalmente, a la nuevas funcionalidades que incorporan los nuevos dispositivos, así como trasladarles las "mejores prácticas" a la hora de hacer uso de los mismos.

PETICIONES

La solicitud de los recursos que supongan coste económico deberán partir siempre de las Direcciones de Servicios de cada Departamento ó, en el caso de otro tipo de organismo integrado dentro de la RCAGV, de la Dirección ó Servicio que se encargue de centralizar todas sus necesidades. Las solicitudes deberán ir acompañadas de toda aquella información necesaria para la resolución de las mismas, acompañada por la firma del máximo representante. Para ello, se ha diseñado un formulario (con formato PDF escribible) que se encuentra disponible en Jakina.

En definitiva, las Direcciones de Servicios u órganos equivalentes serán las responsables de controlar y centralizar las peticiones de sus usuarios departamentales, siempre tratando de ajustar su uso a las necesidades reales. Para ello, las Direcciones de Servicios recibirán periódicamente información sobre el gasto realizado por parte de su Departamento.

Cuadro resumen de las características principales del servicio

Perfil	Plazo de renovación	Teléfono móvil	Roaming	Tipo de línea			Bloqueo por consumo
Alto Cargo	1 año	A elegir entre varios modelos	Asignado por defecto	Internacional, 24 horas + roaming (perfil P1)			Sin bloqueo
Técnico	2 años	Modelo fijo	Asignado bajo petición (con 48 horas de antelación)	Asignado bajo solicitud justificada:			Al llegar al 80% del consumo establecido, el usuario recibe un aviso no restrictivo, y al llegar al 100%, la línea se queda bloqueada para realizar llamadas
				Tipos de perfiles	24 h.	Horario laboral (*)	
				• Internacional	P1B	n/a	
				• Estatal	P2	P3	
				• Comunidad autónoma	P4	P5	
				• Red Privada Virtual	P6	P7	

* El horario laboral abarca el siguiente periodo: de 7 h. a 19:30 h.

RECOMENDACIONES

A continuación, os detallamos algunas recomendaciones para hacer un buen uso del dispositivo móvil:

- **Uso con los portátiles:** Para dotar al portátil de conectividad con Internet y con aplicaciones y recursos de la RCAGV, se establece como estándar el MODEM USB, sin excluir el uso de otras opciones banda ancha, como pueden conexiones de tipo ADSL ó accesos WiFi. Para acceder a aplicaciones y recursos de la RCAGV será necesario, además del Modem USB, la utilización de un cliente VPN (red privada virtual) en el portátil.

Para acceder a servicios instalados en la Intranet de la RCAGV, vía VPN, los usuarios deberán ser internos (corporativos) a la Red de Gobierno, utilizando estaciones de trabajo configuradas bajo la normativa y estándares de la RCAGV.

- **Sincronización:** La única forma validada por el Servicio de Red Corporativa Administrativa para realizar las sincronizaciones de teléfonos móviles será en remoto contra el buzón Microsoft Exchange. Ya que en caso de realizar la sincronización de nuestro portátil contra nuestro cliente Microsoft Outlook mediante cable o cualquier otro medio, la información (contactos, etc.) puede duplicarse e incluso perderse. Por lo tanto, no se permite la sincronización por un medio no validado.
- Dado que cada vez tenemos más aplicaciones en nuestros teléfonos, que los recursos de éstos son limitados, y que su consumo de memoria es cada vez mayor, puede que tengamos bloqueos o indisponibilidad de algunas aplicaciones. Para optimizar su rendimiento, por tanto, se aconseja apagar y encender los dispositivos cada 3 ó 5 días, o ante cualquier síntoma de mal funcionamiento.
- **Transferencias:** una de las funciones más útiles que a partir de ahora se puede utilizar es la posibilidad de hacer transferencias de las llamadas que se reciban en el teléfono móvil.

También es importante no olvidar que todos los terminales son propiedad del operador, y pasado el plazo de cesión (12 ó 24 meses, dependiendo del perfil de la persona), éstos deberán ser devueltos para su sustitución. Por ello, es necesario que mantengamos en buenas condiciones todo el material entregado hasta su devolución: el móvil, el cableado, la caja, etc.

El servicio de Red Corporativa Administrativa entregará al usuario el terminal configurado para poder realizar las tareas de sincronización de datos principales (correo, calendario, contactos), considerando como en otras ocasiones que el repositorio principal de información es el buzón en Exchange (Outlook), siendo ésta la única información sobre la que la Dirección de Informática y Telecomunicaciones tomará responsabilidad.

Los terminales que, en estos momentos, se encuentran disponibles para los Altos Cargos son, entre otros, los siguientes: HTC Touch HD2, Nokia N97, Sony Ericsson Vivaz, HTC Tatoo, Apple iPhone y Samsung GT-I8000 Omnia 2. Los Técnicos, por su parte, disponen de un Nokia E52. La información relativa a los terminales puede ampliarse consultando el documento disponible en Jakina.

INCIDENCIAS Y CATÁLOGO DE SERVICIOS

Recordamos, asimismo, que el Servicio de atención de incidencias responderá a cualquier persona en el teléfono 400 (945.016.400) y a través del correo electrónico siguiente: en el buzón de la libreta de direcciones "*Justicia y Adm. Públ., DIT Telefonía*" o bien en la cuenta de correo dit-telefonia@euskadi.net

Por último, informaros que en breve se publicará, en la intranet Jakina, un **catálogo** detallando todos los servicios comentados en este artículo, así como la forma en la que se pueden solicitar cada uno de ellos y las normas que se deben cumplir. ❑

"El Servicio de atención de incidencias atenderá a cualquier persona en el teléfono 400."

[**+info**]:

Intranet Jakina. Apartado "*Informática y Telecomunicaciones*", sección "*Red Corporativa Administrativa del Gobierno Vasco*"

ALBOAN

¡¡BREVES!!

Nº 39

septiembre de 2010

Barnetegis Tecnológicos

¿Qué es un "*Barnetegi Tecnológico*"? Es un modelo de formación intensivo (suele durar al menos dos días, generalmente fines de semana) cuyo objetivo es adquirir conocimientos de una manera rápida, eficaz y de una forma agradable en el campo de las Nuevas Tecnologías. Se suele realizar aislando a los participantes de su entorno habitual, escogiendo un entorno motivador, como puede ser un entorno natural, junto con personas que tienen idénticos objetivos en lo que respecta al uso y conocimiento de los servicios y herramientas que nos ofrecen las nuevas tecnologías.

De esta forma se van a conocer muchas tecnologías, no sólo de forma aislada, sino que también se intenta enseñar a utilizar estas tecnologías de una forma conjunta.

En cada Barnetegi varios formadores expertos realizan explicaciones y apoyan el trabajo individual de cada asistente. Al final, el objetivo del curso es ser divulgativo y práctico, esto es, dar a conocer a los alumnos las posibilidades existentes y el uso práctico de estas herramientas, y que sean éstos quienes, en función de las técnicas aprendidas y los servicios disponibles en el mundo de las TIC (es decir, las Tecnologías de la Información y de las Comunicaciones más habituales y prácticas a día de hoy), decidan qué herramientas pueden aportar valor a sus equipos de trabajo y a su propio trabajo, en definitiva, utilizar YA las tecnologías.

¿Quiénes son los potenciales alumnos de estos cursos? Generalmente personas que, por su posicionamiento en la empresa, pueden influir dentro de sus organizaciones, por ejemplo, directivos, gerentes… y que perciban las TIC como herramientas útiles para posicionarse en un mercado cada vez más competitivo y cambiante.

¿Cuál es el programa? El programa es variado, y entre otros temas se pueden destacar los siguientes: la Web 2.0, Redes Sociales, dispositivos de última generación, empresa en la Sociedad de la Información, imagen corporativa en Internet, compras on-line, identidad en la red, publicidad en Internet…

Metadatos en las fotos

Después de volver de las merecidas vacaciones de verano muchos de nosotros acumulamos una cantidad importante de fotos, la mayoría en formato digital, que almacenamos en nuestros ordenadores, y que también solemos publicar en Internet (sobre todo en redes sociales), para enseñar a familiares y amigos.

Cuando realizamos esta sencilla acción de publicar fotos en Internet debemos saber que éstas contienen, a parte de la imagen en sí, otra información que está oculta, lo que conocemos como **metadatos** (datos sobre los datos). Estos metadatos se conocen con el nombre de **datos Exif (*Exchangeable image file format*)**.

Exif no es sino una especificación que usa formatos de archivo como JPEG, TIFF o WAVE (formato de audio), entre otros, a los que añade etiquetas (**tags**) como las siguientes:

- Información de fecha y hora de la captura
- Configuración de la cámara (modelo y fabricante, orientación, apertura, velocidad del obturador, distancia focal…)
- Versión Exif usada
- Información sobre la localización (datos GPS), sólo disponible en algunos modelos, por ejemplo el iPhone

Para un formato imagen, los datos Exif están incrustados en el mismo archivo, pudiéndose utilizar programas diversos para leer estos metadatos (por ejemplo ***ExifReader***).

Desde aquí queremos alertar de la información "extra" que estamos dando a cualquier desconocido cuando subimos estos ficheros a Internet. Cabe destacar que **Facebook** elimina esta información cuando se sube una foto a su red social, no siendo ésta la política de otras muchas redes sociales muy populares. Existen herramientas gratuitas (una de ellas es **MetaStripper**) que permiten eliminar, por parte del usuario, estos metadatos.

Sitio no oficial dedicado a la especificación Exif (en idioma inglés): **http://exif.org/**