Instituto Nacional
de Tecnologías
de la Comunicación

INFORME DE VULNERABILIDADES Y AMENAZAS EN DISPOSITIVOS IPHONE E IPAD

INTECO

INTECO-CERT

Enero 2011

Instituto Nacional
de Tecnologías
de la Comunicación

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página http://www.inteco.es.

Instituto Nacional
de Tecnologías
de la Comunicación

ÍNDICE

1. OBJETO DEL ESTUDIO

El avance de las tecnologías móviles se ha convertido en uno de los grandes caballos de batalla de la seguridad de la información. Los dispositivos han pasado de ser simples terminales que permiten la transmisión de voz, a convertirse en verdaderos ordenadores móviles. Su creciente uso, principalmente en entornos corporativos, ha hecho que el puesto de trabajo haya dejado de ser fijo para ganar en movilidad (teléfonos inteligentes, PDA, *Tablets*, portátiles, etc.).

El análisis de estos dispositivos móviles se realiza bajo una nueva dimensión de seguridad ya que, por sus características propias, además de estar expuestos a los mismos riesgos y amenazas que los equipos convencionales -malware, vulnerabilidades, etc.- son susceptibles de robo o extravío con la subsiguiente revelación de información sensible, y daño con la posible pérdida de información crítica para el negocio.

El objetivo de este informe es analizar el estado de la seguridad en los dispositivos iPhone e iPad. Para ello se han identificado y analizando las vulnerabilidad y principales ataques dirigidos que los impactan, aportando enlaces de referencia para su comprensión, mitigación y resolución, en caso de estar disponible.

Por último el informe también incluye buenas prácticas para la protección de los dispositivos así como servicios de INTECO-CERT de utilidad para los responsables de la seguridad de los mismos.

2. AVISOS DE SEGURIDAD

Se ha recopilado la lista de los avisos de seguridad para los dispositivos Apple iPad e iPhone basados en el sistema operativo iPhone OS (IOS). La presente lista no pretende ser una prospección exhaustiva de todas las vulnerabilidades conocidas aunque sí representa las fuentes más importantes de las mismas. La base de conocimiento sobre vulnerabilidades de INTECO recoge **más de 44.500 vulnerabilidades** de diferentes fuentes (NIST, Microsoft, Apple, Adobe, Secunia, etc.).

2.1. AVISOS SOLUCIONADOS

A continuación se listan los avisos de seguridad que corrigen vulnerabilidades del IOS de Apple en sus diferentes versiones estables.

Se listan por fecha descendente.

2.1.1. Vulnerabilidad en Apple iOS para iPhone

- **Fecha de publicación**

8 de Diciembre de 2010

- **Impacto**

Medio 

- **Descripción**

Esta vulnerabilidad se produce en iOS versión 4.0 y 4.1 en dispositivos iPhone.

Se trata de una condición de carrera en Apple iOS 4.0 a 4.1 para iPhone 3G y posteriores permite a atacantes físicamente próximos eludir el bloqueo con código de seguridad realizando una llamada desde la pantalla de llamadas de emergencia y rápidamente presionando el botón de reposo/activación, impacta en la confidencialidad del sistema aunque se minimiza el impacto al poder ser explotado únicamente en local.

El impacto de esta vulnerabilidad es medio.

- **Enlaces**
  - INTECO-CERT
  - Apple

2.1.2. Actualización de seguridad 4.2 para iOS

- **Fecha de publicación**

23 de Noviembre de 2010

- **Impacto**

Medio 

- **Descripción**

Esta actualización de seguridad se encarga de solucionar una serie de vulnerabilidades para versiones anteriores a la 4.2 del sistema operativo iOS.

Esta actualización corrige problemas de seguridad que podrían desembocar en ataque de denegación de servicio (DoS), peticiones no deseadas a servidores remotos, revelación de información confidencial, ejecución de código arbitrario, apagado del dispositivo.

Mediante la aplicación de esta actualización se corrigen 44 vulnerabilidades de impacto medio.

- **Enlaces**
  - INTECO-CERT
  - Apple

2.1.3. Actualización de seguridad para IOS

- **Fecha de publicación**

9 de Septiembre de 2010

- **Impacto**

Medio 

- **Descripción**

Esta actualización de seguridad se encarga de solucionar una serie de vulnerabilidades para versiones anteriores a la 4.1 del sistema operativo iOS

Esta actualización corrige problemas de seguridad que podrían desembocar en ejecución de código arbitrario, redirecciones de llamadas en programas específicos, compromiso del sistema, cambios en el contenido del portapapeles y revelación de información.

La aplicación de esta actualización corrige 24 vulnerabilidades de impacto medio.

- **Enlaces**
  - INTECO-CERT
  - Apple

2.1.4. Actualización de seguridad para IOS

- **Fecha de publicación**

13 de Agosto de 2010

- **Impacto**

Crítico 

- **Descripción**

Esta actualización de seguridad se encarga de solucionar una serie de vulnerabilidades para iOS 4.0.2 y anteriores para dispositivos iPhone y iOS 3.2.2 para los dispositivos iPad

Esta actualización de seguridad corrige problemas de seguridad que permitían ejecutar código arbitrario mediante la visualización de archivos .PDF con fuentes incrustadas manipuladas de forma maliciosa y posibles elevaciones de privilegios del usuario.

Esta actualización corrige 2 vulnerabilidades de impacto crítico.

Estas vulnerabilidades se utilizaban para desbloquear el dispositivo, por lo tanto al aplicar esta actualización los dispositivos pueden perder el desbloqueo y pueden aparecer comportamientos anómalos no documentados ya que la acción del desbloqueo del dispositivo no está soportada por el fabricante.

- **Enlaces**
  - INTECO-CERT
  - Apple
    - iPhone
    - iPad

2.1.5. Múltiples vulnerabilidades en iOS de Apple

- **Fecha de publicación**

22 de Junio de 2010

- **Impacto**

Alto 

- **Descripción**

Este aviso describe una serie de vulnerabilidades para la versión 3 de iOS, este aviso no dispone de parche, sin embargo esto errores se corrigen al actualizar de forma gratuita la versión del sistema operativo a la 4.

Esta actualización de seguridad corrige problemas de ejecución de código arbitrario, revelación de información sensible, denegación de servicio, acceso no autorizado al sistema, ataques de suplantación.

La actualización a iOS 4 corrige 61 vulnerabilidades de impacto crítico.

- **Enlaces**
  - Secunia
  - Apple

2.1.6. Actualización de seguridad para iPhone e iPod touch

- **Fecha de publicación**

3 de Febrero de 2010

- **Impacto**

Medio

- **Descripción**

Esta actualización de seguridad se encarga de solucionar una serie de vulnerabilidades para iOS anteriores a la versión 3.1.3 en dispositivos iPhone.

La actualización corrige problemas de seguridad que pueden producir problemas de finalización de aplicaciones, ejecución de código arbitrario y acceso a información de usuario.

Se corrigen 5 vulnerabilidades de impacto medio.

- **Enlaces**
  - INTECO-CERT
  - Apple

2.1.7. Actualización de seguridad para múltiples vulnerabilidades en iPhone e iPod touch

- **Fecha de publicación**

10 de Septiembre de 2009

- **Impacto**

Alto

- **Descripción**

Esta actualización de seguridad se encarga de solucionar una serie de vulnerabilidades para iOS de la versión 3.1 y 3.1.1 en dispositivos iPhone e iPod Touch.

Dicha actualización corrige problemas de seguridad que pueden desencadenar problemas de suplantación, comprometer la información de usuario aprovechando vulnerabilidades de Cross Site Scripting, exposición de información sensible, denegación de servicio, acceso no autorizado al sistema y ejecución de código arbitrario.

Esta actualización corrige 10 vulnerabilidades de impacto crítico.

- **Enlaces**
  - Secunia
  - Apple

2.1.8. Vulnerabilidad de decodificación de mensajes SMS

- **Fecha de publicación**

3 de Agosto de 2009

- **Impacto**

Alto 

- **Descripción**

Esta actualización de seguridad se encarga de solucionar una serie de vulnerabilidades para iOS de la versión 3.0.1 en dispositivos iPhone.

La actualización corrige un fallo en la decodificación de los SMS por lo que la recepción de uno creado de forma malicioso podría desencadenar problemas de denegación de servicio o acceso no autorizado en el sistema.

Esta actualización corrige 1 vulnerabilidad de impacto crítico.

- **Enlaces**
  - Secunia
  - Apple

2.2. AVISOS NO SOLUCIONADOS

A continuación se listan los avisos de seguridad que identifican las vulnerabilidades del IOS de Apple en sus diferentes versiones estables, y que a día de hoy (17/02/2011), no disponen de solución.

2.2.1. Suplantación de perfiles de configuración en iPhone

- **Fecha de publicación**

4 de Febrero de 2010

- **Impacto**

Bajo 

- **Descripción**

Este aviso afecta a la versión 3 de iOS para dispositivos iPhone.

Se trata de un aviso de seguridad que no reporta ninguna vulnerabilidad pero que se basa en la mala gestión de los ficheros de configuración firmados se comprueban en el almacén de certificados por defecto de Safari, pero no muestra la información del certificado, por lo que se podría suplantar un archivo de configuración para cambiar la configuración del dispositivo.

El impacto de este aviso es bajo.

- **Enlaces**
  - Secunia

3. ESTADO DEL ARTE DE LA SEGURIDAD EN IPAD/IPHONE

Son muchas las noticias que se está generando en torno a la seguridad móvil en los últimos años en parte por el avance de las tecnologías y el aumento exponencial de usuarios.

El talón de Aquiles de estos dispositivos es la confidencialidad, ya que la alta capacidad de almacenamiento con la que se ha dotado a este tipo de dispositivos ha propiciado que los mismos sean utilizados tanto como unidades de almacenamiento así como puestos de trabajo móviles.

El que puedan transportar mayor cantidad de datos los ha convertido en un objetivo potencial para los cibercriminales que intentan obtener acceso a dispositivos e intentar conseguir información sensible, por otra parte al ser dispositivos de alto valor económico son susceptibles de sustracción, lo que provoca grandes problemas de confidencialidad.

En el hilo de este problema se encuentra el problema del acceso no autorizado por un fallo en la implementación de las llamadas de seguridad que permite acceder al teléfono saltando la protección del código de seguridad.

Otros problemas que se han detectado tienen que ver con el phishing ya que el navegador por defecto de estos dispositivos (Safari) al introducir una url y cargar la página la barra de direcciones desaparece, por lo que incluso se han detectado casos de phishing que se aprovechan de esto introduciendo en la página fraudulenta una imagen de la barra de direcciones con una url confiable tratando de engañar al usuario.

Debido a la generalización en el uso de este tipo de dispositivos, se genera mayor investigación de seguridad en sus aplicaciones y sistemas operativos, la consecuencia es que surgen nuevas vulnerabilidades con mayor frecuencia y en mayor número, que podrán derivar en brechas de seguridad.

Algunas de estos agujeros de seguridad son aprovechados para realizar el desbloqueo del dispositivo, conocido comúnmente como <<Jailbreak>>, a su vez el desbloqueo de estos dispositivos se utiliza como vector de ataque, apareciendo malware que simula ser programas para desbloquear el dispositivo, que aprovecha para infectar ordenadores personales e instalarse como troyano robando credenciales bancarias, contraseñas, etc.

Estos desbloqueos a su vez pueden ser utilizados por programas maliciosos aprovechándose de las contraseñas por defecto con las que se instalan.

La solución a este tipo de problemas basados en la liberación del terminar consiste en utilizar siempre fuentes confiables para la descarga del software, en este caso Apple posee una plataforma llamada App Store en la cual únicamente se incorporan herramientas que han sido verificadas por el fabricante.

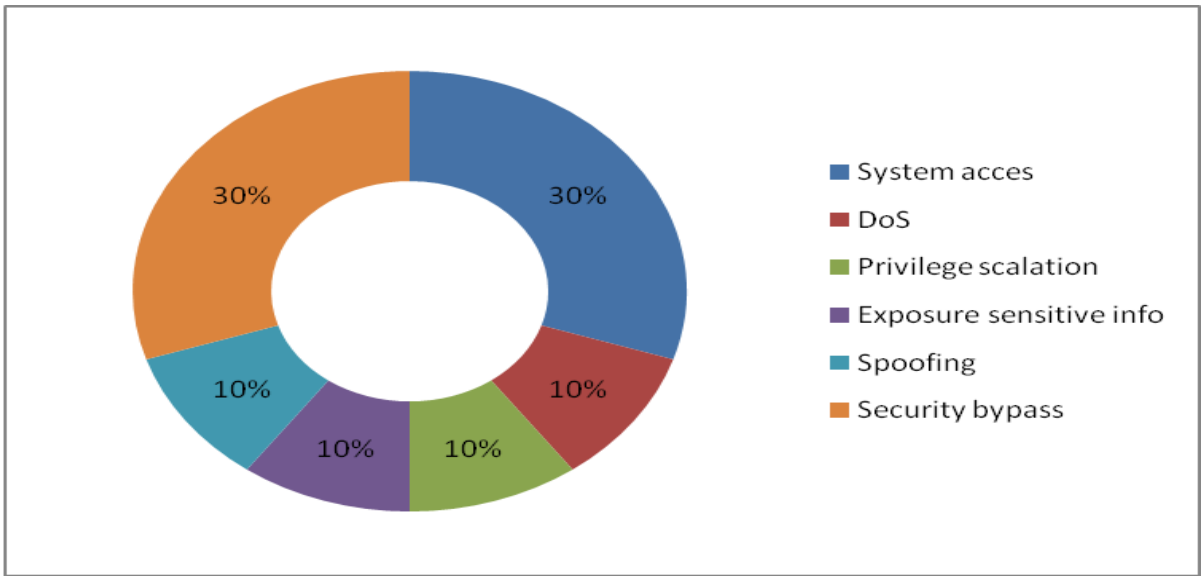
Por otro lado y a raíz de su avance en el mercado comienza a aparecer malware específico para este tipo de dispositivos y las predicciones de las principales empresas de seguridad no ofrecen lugar a dudas, se prevé un gran aumento en este tipo de malware destinado a dispositivos móviles.

Desde INTECO-CERT se ofrecen listados con los virus encontrados para estas plataformas.

4. ESTADÍSTICAS

A continuación se muestran unas gráficas en las que se muestran los principales problemas de seguridad que se han detectado en estos dispositivos para sus distintas versiones.

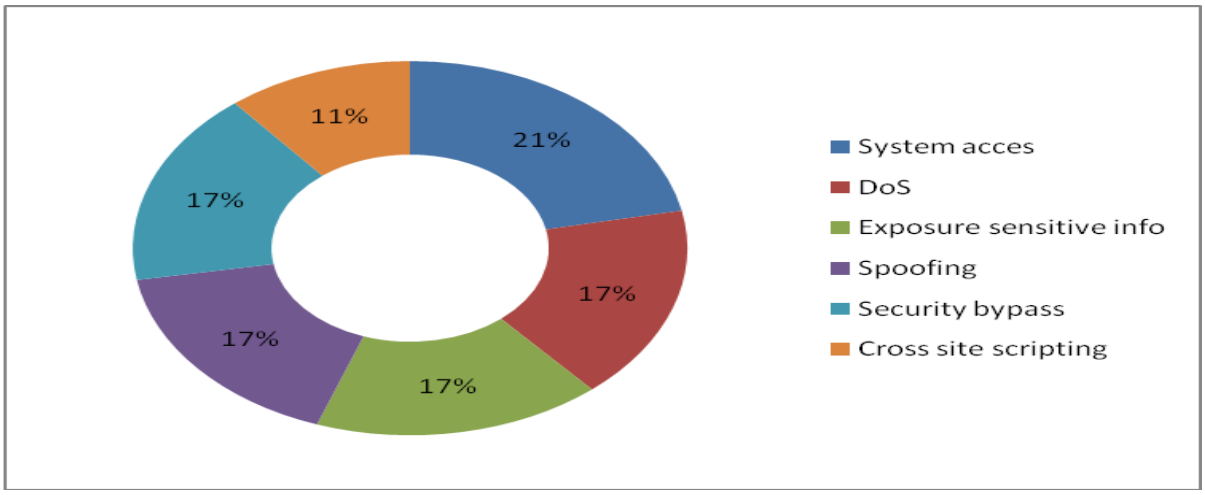
Gráfica 1: Impacto de las vulnerabilidades en iOS 4.X para iPhone



Fuente: INTECO, NIST, Secunia

Como se puede comprobar los principales problemas de seguridad de esta versión de iOS se han centrado en el acceso no autorizado al sistema y evasión de la seguridad implementada en estos dispositivos.

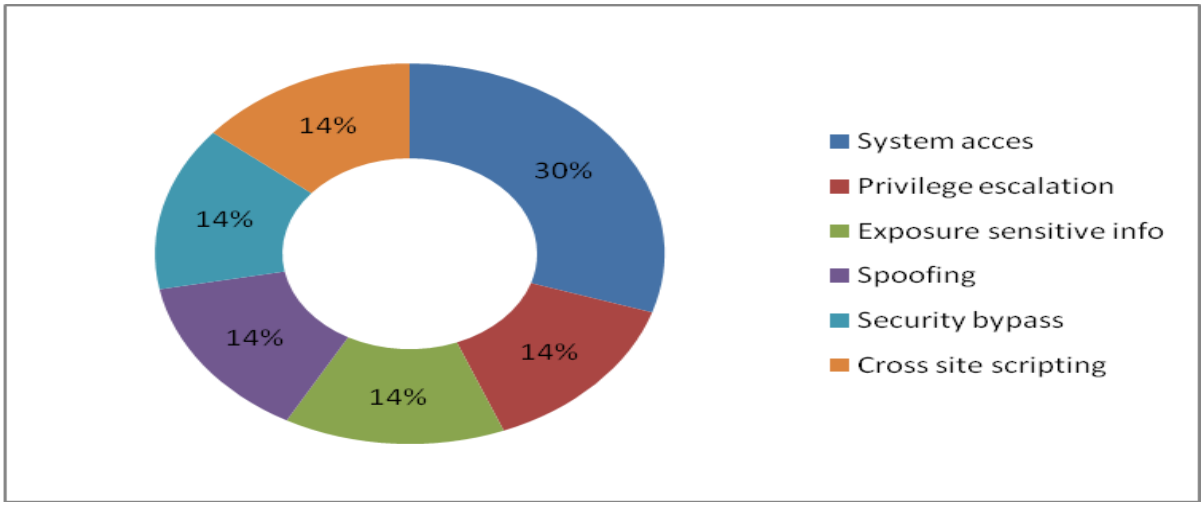
Gráfica 2: Impacto de las vulnerabilidades en iOS 3.X para iPhone



Fuente: INTECO, NIST, Secunia

Para esta versión de iOS se han detectado igualmente problemas de acceso no autorizado al sistema, pero también se producen muchos errores de ejecución de código arbitrario aprovechando vulnerabilidades de cross site scripting, así como denegaciones de servicio y problemas de suplantación.

Gráfica 3: Impacto de las vulnerabilidades en iOS 3.X para iPad



Fuente: INTECO, NIST, Secunia

En los dispositivos iPad con la versión que trae instalada de fábrica la mayoría de los problemas de seguridad desencadenan como consecuencia problemas de acceso no autorizado al sistema, aunque también se producen problemas con la ejecución de código arbitrario mediante la explotación de vulnerabilidades de cross site scripting, evasión de la seguridad y revelación de datos sensibles.

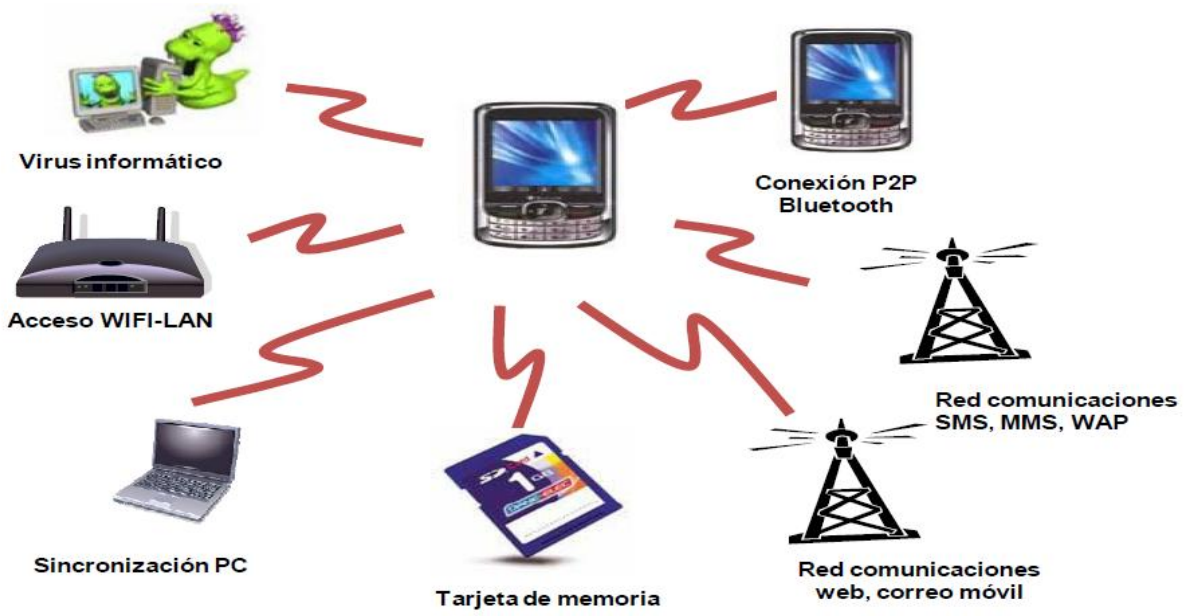
5. RECOMENDACIONES DE SEGURIDAD

Entre los muchos riesgos que entrañan estos dispositivos para la seguridad el más importante es el robo de la información, ya que actualmente estos dispositivos han aumentado su capacidad de almacenamiento exponencialmente, por lo tanto pueden almacenar una gran cantidad de información.

A raíz del aumento de capacidad de estos dispositivos se hace necesario el cifrado de la información del dispositivo, ya que la perdida de los mismos en un entorno empresarial puede producir grandes pérdidas tanto de información como de imagen de empresa.

Los principales focos de infección de estos dispositivos se encuentran en los múltiples canales de comunicación que implementan este tipo de dispositivos.

Imagen 1: Focos de infección de dispositivos móviles



Fuente: INTECO

5.1. ENTORNO DOMÉSTICO

- Utilizar el PIN/password de arranque en el caso de terminales con acceso a la red de los operadores.
- Utilizar las opciones de bloqueo de terminal disponibles en la configuración de estos dispositivos.
- Utilizar programas de cifrado de datos para evitar que la información almacenada en el dispositivo pueda ser leída por una persona ajena.

- Evitar descargar aplicaciones o archivos desde Internet con origen poco confiable. Si se realiza una conexión entre dispositivos (de móvil a móvil, o de móvil a ordenador), comprobar que ninguno de ellos se encuentre comprometido o aloje archivos infectados.

- Configurar el dispositivo para que no se puedan instalar programas que no sean del fabricante sin estar certificados y/o no se conozca la fuente.

- Utilizar software de protección de dispositivos (antivirus).

- No aceptar conexiones de dispositivos que no se conozcan para evitar transferencias de contenidos no deseados.

- Leer los acuerdos de usuario del software que se instalan por si se advierte de la instalación de componentes no deseados (software espía).

- Conectarse únicamente a redes inalámbricas de confianza.

Para más información:

- Guía para proteger y usar de forma segura su móvil.

5.2. ENTORNO CORPORATIVO

Además de las indicadas para el usuario doméstico se deberán tener en cuenta otras recomendaciones:

- Recurrir a sistemas de gestión centralizada de dispositivos, que posibilitan el bloqueo y borrado remoto de información en caso de pérdida o robo del terminal móvil, el control remoto del software instalado por los usuarios y su borrado en caso de que no cumpla las políticas de seguridad establecidas por la empresa.

- Aplicación de las políticas de seguridad de los sistemas operativos. Utilización del software original, de forma que se puedan realizar las actualizaciones de seguridad pertinentes y recurrir a los departamentos de atención al cliente que dichas empresas tienen para ayudar a definir medidas de seguridad adecuadas a las pymes.

6. SERVICIOS DE INTECO-CERT

INTECO-CERT dispone de varios servicios que pueden ser de utilidad para la gestión de la seguridad de la información de los dispositivos iPhone e iPad.

6.1. BOLETINES DE SEGURIDAD Y VULNERABILIDADES

6.1.1. Boletín de avisos de seguridad

Los boletines de avisos incluyen la última hora sobre las amenazas más relevantes, adecuadas tanto en la complejidad técnica como en las temáticas a cubrir para diferentes perfiles -técnico y no técnico- con información práctica de actualidad que facilita la prevención, protección y respuesta ante incidentes de seguridad.

- **Avisos técnicos.** Enfocados a usuarios con un perfil técnico avanzado, como pueden ser administradores de sistemas y responsables de seguridad, cubre amenazas y vulnerabilidades en aplicaciones de uso generalizado en entornos corporativos.
- **Avisos no técnicos.** Enfocados a internautas cubre vulnerabilidades en aplicaciones de uso generalizado - sistema operativo, navegadores, reproductores multimedia, terminales móviles... -, nuevos intentos de fraude, correos potencialmente peligrosos o de alarma social, entre otros.

6.1.2. Boletín de vulnerabilidades

INTECO, mediante un acuerdo de colaboración con el NIST y su base de datos de vulnerabilidades NVD (National Vulnerability Database), pone a disposición del público hispanohablante a través de INTECO-CERT su base de datos en castellano con información sobre cada una de las vulnerabilidades informáticas públicamente conocidas.

INTECO dispone de un servicio de gestión de vulnerabilidades a través de un boletín de vulnerabilidades, el cual está enfocado a administradores de sistemas y **permite filtrar los productos de los que recibir las notificaciones**, en el instante en el que una vulnerabilidad afecta a alguno de los productos seleccionados se envía una notificación por correo con toda la información disponible.

6.1.3. Boletín de actualidad

Recoge diariamente las notas de actualidad, noticias, virus y eventos con los que estar al día de lo más relevante en el ámbito de la seguridad. Permite **personalizar el boletín filtrando los virus por las plataformas a las que afectan**: Apple Mac OS, GNU/Linux, Móviles, Microsoft Windows y Otros.

Para hacer uso de los servicios de Boletines es **necesario ser un usuario registrado del portal de INTECO**. La forma de acceder al apartado de Suscripción de boletines es, dentro de la opción de “Editar Perfil”, accediendo en el menú izquierdo a la sección: Servicios comunes -> Servicios opcionales para todos los usuarios.

6.2. GESTIÓN DE INCIDENTES DE SEGURIDAD

INTECO-CERT ofrece también un servicio de asistencia y soporte desde el cual se puede solicitar asistencia ante un incidente de seguridad, para ello dispone de un equipo especializado en el análisis y gestión de incidentes de seguridad.

El servicio se presta a través de correo electrónico, disponiendo a tal efecto de la dirección INCIDENCIAS@CERT.INTECO.ES

Si el incidente requiere intercambio de información sensible las comunicaciones por correo se realizaran cifradas con PGP, estando disponible la clave pública en http://cert.inteco.es/Acerca_de/Claves_publicas_PGP/

6.3. ANÁLISIS DE MALWARE

En **investigaciones de incidentes** que así lo requieran **o nuevas amenazas**, el equipo técnico de INTECO-CERT realiza **análisis de malware**, tanto en ejecución, para conocer mejor el comportamiento del miso como en estático, utilizando técnicas de ingeniería inversa.

Estos análisis pueden ser de malware tanto de malware diseñado para afectar a plataformas de servidor o escritorio, como a plataformas móviles, puesto que cada vez se están dando más casos de amenazas especialmente dirigidas a estas plataformas.

6.4. ANÁLISIS FORENSE EN CASO DE INCIDENTE

Al igual que en el caso anterior, en los incidentes que requieran un **análisis forense detallado** que permita **determinar el origen del mismo y las consecuencias en los sistemas afectados**, el equipo de INTECO-CERT dispone de otro servicio bajo demanda de análisis forense.

En este servicio se realizará un clonado y posterior análisis pormenorizado del sistema o sistemas afectados, manteniendo siempre la cadena de custodia adecuada en estos casos. Al igual que en el caso anterior es un servicio que aplica tanto a sistemas servidor, de escritorio, como a dispositivos móviles.