Desarrollo de un servicio integral de gestión del segmento de cuarentena en una red de ordenadores

Development of a comprehensive service to set up quarantine segments in computer networks

Miquel Bordoy, Ricardo Díaz, Antoni Sola

Resumen

En una red de área local (LAN, Local Area Network), la presencia de dispositivos infectados con algún tipo de malware, en manos de usuarios maliciosos, sin cumplir la política de seguridad de la institución (sin antivirus, con sistemas sin actualizar, configuraciones de red incorrectas, servicios de red abiertos, etc.), representa un serio peligro para el resto de dispositivos y recursos corporativos disponibles en ella, y para el propio servicio de red.

En las redes de hoy en día existen diferentes formas de detectar estos dispositivos conflictivos, con un correlador de eventos de seguridad, con un sistema de detección/prevención de intrusos (IDS/IDP), a partir de los registros de un cortafuegos, etc. Aunque se disponga en la red de los más avanzados sistemas de detección, de poco servirán si no se instaura en la red un servicio de gestión de estos ordenadores conflictivos que se encargue, entre otros, de localizar y aislar automáticamente el ordenador conflictivo, y de notificar de forma electrónica y automatizada las incidencias a los usuarios.

En este artículo se pretenden mostrar los resultados de los trabajos y desarrollos realizados en este campo por el Centro de Tecnologías de la Información de la Universitat de les Illes Balears (UIB). La solución propuesta se basa en la combinación de estándares de networking y, por tanto, encaja perfectamente en cualquier infraestructura de red de área local de los principales fabricantes. Además, la solución se construye sólo con conocidos proyectos open source (freeradius, mysql, iptables, Apache web server, dhcpd, etc.) y es independiente del sistema operativo del dispositivo del usuario.

Palabras clave: MAC (Media Access Control) Authentication, Dynamic VLAN (Virtual LAN), Network Access Control (NAC), Quarantine VLAN, Trusted Network Connect (TNC).

Summary

In a LAN (Local Area Network), the presence of infected devices with some type of malware, in the hands of malicious users, without complying the security policy of the institution (without antivirus, not updated operating system, incorrect network settings, unused network services activated, etc.), etc. represents a serious risk to the rest of devices and corporate resources and to the service network as well.

In today's data networks there are different ways to detect these troubled devices: with a security event correlator, with an intrusion detection/prevention system (IDS/IDP), from the firewall logs, etc. Although the network has the most advanced detection systems, these are of little use without deploying a network service to manage troubled computers. This new service should allow not only network location and automatic isolation of troubled computer but also automated electronic reporting of incidents to users.

This paper is intended to show the results of the work and developments in this field conducted by the Information Technology Center at the Universitat de les Illes Balears (UIB). The proposed solution is based on the combination of networking standards and, therefore, it fits perfectly into any local area network infrastructure from the main manufacturers. Furthermore, the solution is built only with known open source projects (freeradius, mysql, iptables, Apache web server, dhcpd, etc.) and it is operating system independent user's device

Keywords: MAC (Media Access Control) Authentication, Dynamic VLAN (Virtual LAN), Network Access Control (NAC), Quarantine VLAN, Trusted Network Connect (TNC).

La presencia de dispositivos infectados en una red local representa un serio peligro para el resto de dispositivos

La solución propuesta se basa en la combinación de estándares de networking

1. Introducción: la versión electrónica del lazareto

En el año 1817 finalizó la construcción del Lazareto de Mahón sobre una pequeña península situada en la entrada del puerto de Mahón, en la isla de Menorca[1]. En aquella época, la finalidad de los lazaretos era el de albergar temporalmente las personas, las embarcaciones y las mercancías que llegaban por mar procedentes de otros lugares con presencia o sospecha de enfermedades infecciosas. En estos terrenos aislados se mantenían en cuarentena estos entes y en caso de detectar alguna infección o contagio se aplicaba el remedio correspondiente. De esta forma, se resguardaba la salud pública de los lugareños, ya que no se daba entrada a las personas o mercancías hasta confirmar que estaban libres de contagio.

Transcurridos casi dos siglos desde la puesta en marcha del Lazareto de Mahón, esta misma necesidad existe hoy en día en las redes de ordenadores. En las redes de área local se comparten recursos multitud de dispositivos y, por tanto, la presencia de un ordenador conflictivo, por ejemplo infectado con un virus, puede provocar la propagación del virus a través de la red y contagiar al resto de dispositivos. Sin la implantación en la red de un "lazareto electrónico", que aísle a estos ordenadores y los mantenga en cuarentena hasta liberarlos de todo contagio, la gestión de estos ordenadores se convierte en una ardua tarea y pone en serio peligro la integridad de todos los recursos en red.

El trabajo se centra en la definición y desarrollo de un sistema para la gestión automática de un lazareto electrónico

El trabajo aquí expuesto se centra en la definición y desarrollo de un sistema para la gestión automática de un lazareto electrónico. En él se albergará temporalmente a los ordenadores de puesto de trabajo conflictivos (infectados con malware, con configuraciones incorrectas y/o inseguras, en manos de usuarios maliciosos, etc.); es decir, ordenadores que no están en condiciones de conectarse a la red (sin antivirus, con el sistema sin parchear, con servicios innecesarios abiertos, etc.) o ordenadores que representan un peligro para el resto de dispositivos conectados a la red y para los servicios que en ella se ofrecen, incluido el propio servicio de red.

La motivación inicial del proyecto fueron los resultados no del todo satisfactorios con la implantación de un lazareto electrónico no automatizado en la Universidad. Con el objetivo de identificar sus puntos débiles se describe el proceso dedicado a gestionar los ordenadores de puesto de trabajo conflictivos:

El objetivo era identificar los puntos débiles del lazareto electrónico

1. El operador de seguridad, a partir de alguna herramienta, detecta la presencia en la red de un ordenador conflictivo y registra una nueva incidencia de seguridad en el sistema de gestión de incidencias corporativo.
2. El operador de red recaba el máximo de información posible del dispositivo y lo localiza en la red (puerto y conmutador de red en el cual se encuentra conectado).
3. Seguidamente, el operador de red aísla el ordenador de la red.
4. El operador de helpdesk o microinformática, a partir de la incidencia reportada, contacta con el usuario del ordenador para intentar solucionar el problema.
5. Tras finalizar su intervención, el operador de microinformática contacta con el operador de red para que reestablezca el servicio de red al ordenador en cuestión.
6. El operador de red desaísla de la red el ordenador.
7. El operador de seguridad verifica que la incidencia no se vuelve a reproducir y la cierra.

Este sistema es ineficiente, incompleto, poco ágil y, entre otros, manifiesta los siguientes problemas:

1. La localización del ordenador en la red, si no se dispone de las herramientas adecuadas, consume un tiempo que puede resultar clave en incidencias con alta criticidad.

2. El método usado para aislar de la red un dispositivo es la desactivación manual y remota del puerto del conmutador en el cual se encuentra conectado. Al desactivar el puerto de red, el usuario detecta que no funciona la red y puede que reaccione conectando el ordenador a otra toma de red (a otro puerto) o puede que solicite el alta en red de alguna otra toma. En este caso, el ordenador reestablecería el servicio de red sin haber subsanado su problema. Además, se volvería a generar otra incidencia con el mismo dispositivo y se tendría que desactivar otro nuevo puerto. En resumen, se puede llegar a situaciones de total descoordinación entre operadores y usuarios finales.

3. En algunas ocasiones se desconoce el usuario del ordenador conflictivo y, por tanto, para solucionar el problema debe personarse in-situ algún operador de microinformática. Además, si no se dispone de un inventario actualizado de puertos-tomas-espacios, esta tarea suele requerir mucho tiempo.

En ocasiones se desconoce el usuario del ordenador conflictivo

4. Al encontrarse aislado su ordenador, el contacto con el usuario final por vía telefónica es la única opción posible pero puede darse el caso que éste no se encuentre en su puesto de trabajo. Esto dificulta el trabajo de los operadores de microinformática, aumenta considerablemente el tiempo medio de resolución de incidencia y se acumula un gran número de incidencias pendientes de resolver.

5. Los usuarios no suelen tomarse muy bien la desactivación completa del acceso a red de su ordenador y en algunos casos lleva a situaciones desagradables. Este hecho se agrava si tiene aislado su ordenador desde hace un tiempo porque, por ejemplo, no se le ha podido comunicar su incidencia.

6. Si el aislamiento consiste en la desactivación del puerto LAN, se dificulta la intervención del operador de microinformática ya que no puede acceder de forma remota al ordenador. Una solución es acudir a la propia ubicación del ordenador, con la gran dedicación de recursos que esto implica al servicio de helpdesk. Otra solución es volver a activar el puerto para poder acceder remotamente al ordenador e intentar solucionar la incidencia. En este caso, se reproducirá la incidencia mientras ésta se intenta solucionar, y en la mayoría de casos esta situación no es admisible.

Si el aislamiento consiste en la desactivación del puerto LAN, se dificulta la intervención del operador de microinformática

7. Para resolver las incidencias, en la mayoría de casos se requiere que el ordenador tenga acceso a algunos recursos en red como, por ejemplo, el servidor de actualizaciones del sistema operativo Microsoft Windows, el servidor de antivirus corporativo, el repositorio de software, etc. En caso de estar completamente aislado, la solución del problema resultará ser menos ágil y, por consiguiente, aumentará considerablemente el tiempo dedicado a su resolución.

Hoy en día cohabitan en la red multitud de herramientas y dispositivos para la detección de ordenadores conflictivos: desde el análisis de logs, o registros, de un cortafuegos o de un IDP (Intrusion Detection and Prevention), hasta las alarmas reportadas por un correlador de eventos de seguridad e incluso por la notificación de una incidencia de seguridad desde un CERT (Computer Emergency Response Team). Aunque la red disponga de estos elementos, de poco servirán si no se implanta un lazareto electrónico automatizado que permita abordar eficientemente la resolución de estas incidencias.

En el momento de abordar este proyecto no existía ninguna solución de terceros, ni de fabricante hardware/software, ni open source, que se adaptase a las necesidades particulares definidas y, por tanto, se optó por la definición y desarrollo de este nuevo servicio de red. En el siguiente apartado se describe el nuevo modelo de lazareto electrónico que soluciona la problemática a partir del aislamiento automático de los ordenadores en una red de área local virtual, o VLAN, de cuarentena y de la implantación de un sistema de notificación automatizado que informe eficientemente al usuario de la incidencia de seguridad con su dispositivo.

2. Un modelo de lazareto electrónico

El modelo de lazareto electrónico propuesto pretende solucionar toda la problemática descrita anteriormente e identificada como resultado de la experiencia en la gestión de ordenadores conflictivos, basada en un modelo manual. La **figura 1** representa gráficamente el escenario sobre el cual se implanta la versión electrónica del lazareto. En él se identifican los diferentes tipos de usuarios que interaccionan con el sistema y los elementos sobre los cuales éste se construye. El objetivo de este apartado es describir en detalle este escenario y la interacción entre los diferentes elementos involucrados desde la creación de una incidencia hasta su resolución.

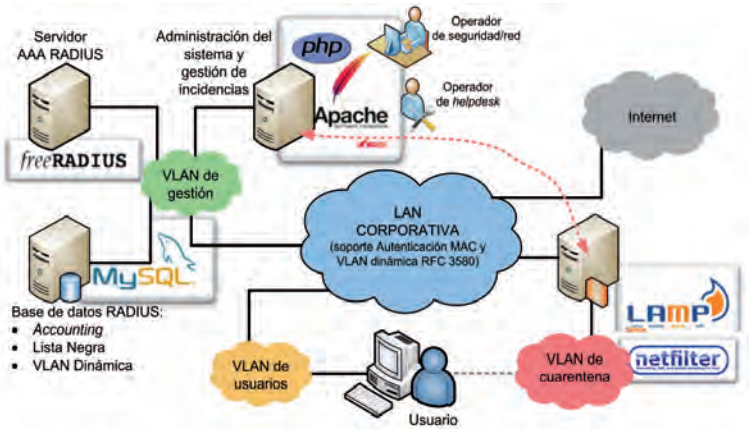
En el nuevo modelo propuesto los usuarios pueden clasificarse en tres grupos

En el apartado anterior, al describir el modelo tradicional, ya se han identificado cuatro tipos de usuarios: el propio usuario responsable del ordenador conflictivo y los operadores de seguridad, red y microinformática. En el nuevo modelo propuesto, al automatizar en el propio sistema ciertas tareas, los usuarios pueden clasificarse sólo en tres grupos:

- Operador de seguridad: encargado de detectar en la red ordenadores conflictivos y registrar en el sistema estas incidencias de seguridad. Este papel también lo podría desempeñar un agente software y, de esta forma, se automatizarían también sus funciones.
- Operador de helpdesk o microinformática: persona del servicio de helpdesk encargada de solucionar las incidencias. Según el tipo de incidencia, el sistema propuesto también permite que el mismo usuario la solucione sin la intervención de este operador, con los consiguientes ahorros que ello implica.
- Usuario: usuario responsable del ordenador de puesto de trabajo con alguna incidencia de seguridad reportada.

El operador de microinformática se encarga de solucionar las incidencias

FIGURA 1. ESCENARIO DEL LAZARETO ELECTRÓNICO



Cada uno de estos tres tipos de usuarios desempeña su papel en el escenario propuesto de lazareto electrónico. Estos usuarios pueden interaccionar entre ellos y con diferentes elementos del escenario. Tal como muestra la **figura 1**, en el modelo de lazareto electrónico se diferencian los siguientes elementos:

- Red de área local, o LAN (Local Area Network), segmentada en diferentes redes virtuales o VLANs (Virtual LAN). Entre las diferentes VLANs dedicadas a ordenadores de usuarios se identifica una VLAN de cuarentena que alberga temporalmente los ordenadores conflictivos de las otras VLANs.
- Servidor AAA (Authentication, Authorization and Accounting) RADIUS (Remote Authentication Dial In User Service) estandarizado por el IETF (Internet Engineering Task Force) principalmente en la RFC (Request For Comments) 2865 y en otras relacionadas[2]. Elemento encargado de mantener una lista negra con los ordenadores conflictivos que por razones de seguridad deben migrarse a la red, o VLAN, de cuarentena del lazareto electrónico. También se encarga de mantener un registro histórico que permitirá conocer, en cualquier instante de tiempo, en qué conmutador de red y puerto se ha conectado cualquier ordenador de la LAN.
- Electrónica de red de acceso con conmutadores Ethernet que soportan autenticación de ordenadores basada en su dirección MAC (Media Access Control), o dirección física de capa de enlace, (MAC Authentication) y asignación dinámica de VLAN (VLAN Authorization) vía RADIUS (segúnRFCs 3580[3] y 2868[4]).
- Aplicativo de administración del sistema y de gestión de incidencias de seguridad. Permite a los operadores de seguridad y helpdesk gestionar las incidencias y administrar otros aspectos del sistema.
- Portal cautivo encargado de aislar y controlar el tráfico de red entre el segmento de cuarentena y la red de la institución. Se encuentra enlazado al sistema gestor de incidencias y construye sus páginas web dinámicamente en base a esta fuente de información de incidencias. El sistema aprovecha su interfaz web como medio de comunicación con el usuario. Incluye un repositorio propio con todo tipo de software (antivirus, vacunas, actualizaciones de sistema, etc.) que en algunos casos permitirán que el propio usuario pueda solucionar fácilmente sus incidencias.
- Aplicaciones u otros repositorios, como, por ejemplo, el servidor de antivirus corporativo o el servidor local WSUS (Windows Server Update Services), sincronizado con los oficiales del fabricante, que deberán ser accesibles, de forma segura y controlada, desde el segmento de cuarentena.

El servidor AAA se encarga de mantener una lista negra con los ordenadores conflictivos

Presentados los diferentes tipos de actores y el escenario del lazareto electrónico, se describe su funcionamiento a partir del circuito completo que seguiría una incidencia en el modelo propuesto. El proceso se inicia con la detección por parte del operador de seguridad de la existencia de un ordenador conflictivo que con su presencia pone en peligro la integridad del resto de recursos en red. Para evitar esta situación no deseada, el operador registra una nueva incidencia en el sistema informando de la dirección física ethernet, o MAC, del ordenador y otros datos que pueden resultar de interés para su posterior resolución, como, por ejemplo, una descripción del problema que padece. Además, en caso de tratarse de un problema con un remedio ya conocido, el mismo operador puede indicar al sistema la vacuna, actualización u otro remedio que debe presentarse al usuario para facilitar la resolución.

El operador registra una nueva incidencia informando de la dirección física ethernet, o MAC, del ordenador

El sistema, al registrarse la nueva incidencia, automáticamente localiza el ordenador en la red (a partir del accounting del servidor RADIUS que contiene el histórico de asociaciones MAC-Puerto de red) y lo conecta a la red de cuarentena añadiendo su dirección MAC en la lista negra del servidor RADIUS. Además, para asegurar que en el mismo instante el dispositivo quede aislado en la red de cuarentena, el sistema contacta con el conmutador, a través del protocolo de gestión estándar SNMP (Simple Network Management Protocol), y provoca la reautenticación MAC del puerto de red en el cual se encuentra conectado.

En este momento, el ordenador conflictivo se encuentra aislado en el segmento de red de cuarentena sin tener conectividad con el resto de la red. Sólo en el caso de incidencias de seguridad graves el ope-

rador de helpdesk será quien contacte con el usuario del ordenador. En la mayoría de los casos, el servicio de microinformática no tratará la incidencia hasta que el usuario contacte con dicho servicio. Éste será informado de la necesidad de tratar tal incidencia de su ordenador al intentar acceder con cualquier navegador web a cualquier página. El portal cautivo del segmento de cuarentena interceptará esta petición web y presentará en su lugar una página web informativa totalmente personalizada en la cual se notificará la incidencia (identificador, descripción, estado, etc.), se informará de la forma de contactar con el servicio de helpdesk y opcionalmente se presentará al usuario un formulario para recoger más datos (nombre de usuario, teléfono, localización, dirección e-mail, etc.) y, cuando sea posible, el remedio al problema.

Suponiendo que ya existe la comunicación entre el usuario y el servicio de microinformática, el paso siguiente consiste en que éste último se encargue de solucionar el problema. En algunos casos, la solución puede ser tan simple como activar algún remedio software para que el usuario lo descargue desde el mismo portal cautivo. En otros casos, el operador deberá activar temporalmente cierto tráfico de red entre el ordenador conflictivo y otros recursos de la red; por ejemplo, para establecer una sesión remota sobre él o para permitirle actualizar su aplicativo antivirus o su sistema Microsoft Windows desde los servidores de la institución.

Una característica muy relevante de esta propuesta es que no depende de funcionalidades propietarias de los fabricantes de networking

Tras completarse la resolución del problema, el operador de helpdesk registrará la incidencia como resuelta y el sistema automáticamente lo eliminará de la lista negra del servidor RADIUS para seguidamente provocar la reautenticación del puerto de red y así devolver inmediatamente el ordenador a su correspondiente VLAN.

Con el modelo propuesto se solucionan los siete aspectos de la problemática asociada al modelo tradicional de gestión de dispositivos conflictivos presentado en el apartado introductorio. Una característica muy relevante de esta propuesta es que sólo se basa en estándares y, por tanto, no depende de funcionalidades propietarias de los fabricantes de networking. Además, se consigue instaurar en la red un nuevo servicio ágil, eficiente y automatizado que permite mejorar el tiempo de respuesta en la resolución de este tipo de incidencias, salvaguarda el resto de recursos de la red, consume menos recursos humanos del servicio de microinformática y mejora considerablemente la satisfacción de los usuarios ante este tipo de incidencias con sus ordenadores. Los aspectos más técnicos que permiten implantar el lazareto electrónico en la red se presentarán en el siguiente apartado.

Uno de los principales requisitos del proyecto es el uso de estándares de networking y la utilización de open source

3. Desarrollo e implementación de un lazareto electrónico

El modelo propuesto de lazareto electrónico define el escenario, o infraestructura, sobre el cual se implanta, los diferentes tipos de actores que participan en él y su funcionamiento. En el mercado existen algunos productos que solucionan algunas de las problemáticas expuestas, pero ninguno de los analizados en los inicios del proyecto permite implantar en la red el modelo de lazareto electrónico que se perseguía en este trabajo. En el presente apartado se describe cómo se ha desarrollado e implementado el modelo, sin nunca perder de vista uno de los principales requisitos del proyecto: el uso de estándares de networking y la utilización en la medida de lo posible de programario open source.

Desde el punto de vista de la electrónica de red de acceso, la implantación del lazareto electrónico únicamente requiere que ésta soporte la segmentación de la red con VLANs, la autenticación de los dispositivos a través de su dirección MAC vía un servidor RADIUS y la asignación dinámica de VLAN a través del mismo servicio AAA.

Como servidor RADIUS se ha utilizado en el proyecto FreeRADIUS[5]. Actualmente ésta es la solución RADIUS open source más extendida y estable. Las tres A's de este servicio se utilizan para verificar si los dis-

positivos que se conectan a la red están en la lista negra de ordenadores conflictivos (Authentication), para aislar dinámicamente estos ordenadores en la red virtual de cuarentena (Authorization) y para mantener un registro de los ordenadores que se han conectado a la red, en qué instante, hasta cuándo, por qué puerto, de qué conmutador, etc. (Accounting).

Este triple servicio AAA se apoya en la conocida y extendida solución open source de base de datos: MySQL[6]. Este repositorio, que almacena la lista negra y todo el accounting, puede ubicarse en el mismo servidor AAA o, mejor, en otro servidor dedicado a mantener este gestor de base de datos, configurado y administrado por técnicos especializados y salvaguardado con su propio sistema de respaldo.

Otro elemento primordial de esta infraestructura es el portal cautivo, ubicado entre el segmento de cuarentena y la red institucional. Existen algunas soluciones open source, pero ninguna de ellas se adaptaba por completo a las necesidades del proyecto y, por este motivo, se optó por el desarrollo de uno propio. La implementación de este portal se basa en la combinación de LAMP (Linux, Apache HTTP server[7], MySQL y PHP[8]) con otras soluciones open source como el cortafuegos Iptables[9], el servidor DHCP (Dynamic Host Configuration Protocol) dhcpd del ISC[10] y el proxy ARP (Address Resolution Protocol) farpd[11]. Un aspecto muy importante del portal cautivo desarrollado es su gran flexibilidad en cuanto a la inclusión de nuevas funcionalidades adaptadas a las necesidades y al entorno de la institución.

El portal cautivo está ubicado entre el segmento de cuarentena y la red institucional

FIGURA 2. NOTIFICACIÓN DE INCIDENCIA POR PORTAL CAUTIVO

El servidor web que incorpora construye dinámicamente sus páginas web

Las principales funciones del portal cautivo ya se han identificado en el apartado anterior. El servidor web que incorpora construye dinámicamente sus páginas web (a partir de la base de datos de incidencias) a través de las cuales se notifica de forma personalizada las incidencias de seguridad a los usuarios (ver la **figura 2**). Por su parte, el cortafuegos Iptables es el encargado de redireccionar a este servicio web cualquier solicitud HTTP realizada desde el segmento de cuarentena y, además, controla el tráfico de red entre este segmento y la red de la institución. Además, el desarrollo de algunos scripts permite a los operadores de microinformática, durante la resolución de la incidencia, modificar de forma gráfica y sencilla el comportamiento del cortafuegos para poder establecer una sesión remota sobre el ordenador conflictivo o para permitirle el acceso a algún recurso corporativo como, por ejemplo, el servidor de actualizaciones WSUS.

Los módulos dhcpd y farpd integrados en el portal cautivo tienen como finalidad resolver la problemática del direccionamiento IP de los ordenadores conflictivos que residen en el segmento de cuarentena. El

servidor DHCP implantado con el demonio dhcpd configura dinámicamente el protocolo IP (dirección IP, máscara de subred, puerta de enlace y servidor de nombres DNS) a los ordenadores sin dirección IP fija. En cambio, el demonio farpd implementa un servicio de Proxy ARP que permite a los ordenadores con dirección IP fija poder tener conectividad con el portal cautivo aunque formen parte de una red IP diferente. Además, el acceso de estos ordenadores a recursos externos de la red de cuarentena también es posible configurando adecuadamente el estándar NAT (Network Address Translation) en el cortafuegos del portal cautivo.

Tanto el portal cautivo como el servidor RADIUS hacen uso de la base de datos de incidencias. El lazareto electrónico incluye un aplicativo web para la administración del sistema y la gestión de incidencias orientado a este tipo de escenarios. Tal aplicativo se ha desarrollado en el entorno LAMP junto con la solución open source de correo electrónico postfix[12]. El operador de seguridad genera y realiza un seguimiento de las incidencias en este aplicativo. Por su parte, el operador de microinformática accede al aplicativo para conocer el estado de las incidencias, para obtener más información de ellas (dirección IP y localización en red del ordenador, si actualmente está conectado a la red, datos de contacto del usuario responsable, etc.) y para cerrar las incidencias resueltas.

El portal cautivo y el servidor RADIUS hacen uso de la base de datos de incidencias

A partir de este aplicativo los operadores podrán personalizar, para cada incidencia, la página web del portal cautivo para que incluya la descarga de cualquier archivo que pueda ayudar en la resolución del problema (por ejemplo, alguna vacuna, una versión actualizada del antivirus corporativo, algún aplicativo para establecer un control remoto sobre el ordenador, etc.). Además, se ha integrado al aplicativo el escáner de vulnerabilidades de seguridad open source Nessus[13], que permite en algunos casos realizar este tipo de testeos sobre el ordenador en cuarentena, desde el mismo portal cautivo, con el fin de realizar una valoración de las posibles causas de la incidencia.

En algunos casos puede resultar indispensable evitar que ciertos dispositivos de la red, aunque puedan parecer conflictivos, pasen a formar parte del segmento de cuarentena (teléfonos IP, impresoras, algún servicio no corporativo, etc.). El aplicativo implementa esta funcionalidad de protección contra la cuarentena gestionando una lista anti-cuarentena y notificando al servicio de microinformática de la presencia en la red de alguno de estos dispositivos.

Como puede comprobarse, los módulos software de terceros sobre los cuales se ha implantado el modelo son todos ellos conocidos proyectos open source. Esta importante característica dota al lazareto electrónico de una continuidad asegurada y de una gran flexibilidad respecto a la inclusión de nuevas funcionalidades. Además, el enorme esfuerzo económico que supuso la construcción del Lazareto de Mahón no tiene su traducción en su versión electrónica, hecho que abre aún más las puertas a la implantación de este servicio en una red de área local.

El enorme esfuerzo económico que supuso la construcción del Lazareto de Mahón no tiene su traducción en su versión electrónica

4. Conclusiones

En la actualidad existen diversas formas de detectar ordenadores conflictivos conectados a la red. De hecho, en la mayoría de redes conviven cortafuegos, IDPs, gestores de ancho de banda, correladores de eventos de seguridad, servidores de antivirus, etc., dispositivos a partir de los cuales puede detectarse su presencia en la red.

Por contra, actualmente existe un importante hueco por cubrir en lo referente a la gestión de estos ordenadores con incidencias de seguridad, desde su detección hasta la solución final de la incidencia, pasando por su localización en la red y su aislamiento en un segmento de cuarentena. Además, esta gestión debe incluir un adecuado sistema de notificación de incidencias a los usuarios y su integración con el gestor de incidencias corporativo.

En el trabajo aquí expuesto se define un modelo para la gestión completa de esta problemática a partir de la experiencia adquirida a lo largo de los años. Con el apoyo de la tecnología adecuada descrita anteriormente se ha logrado desarrollar un sistema real, basado en el modelo, que puede implantarse en la mayoría de redes de área local, con el único requisito para los ordenadores cliente de la presencia de un navegador web y con la ventaja de que los componentes o módulos de terceros usados son open source.

El sistema final desarrollado goza de una gran flexibilidad. Esta característica ha permitido que en los procesos de desarrollo y de evaluación de su implantación se hayan ideado nuevas funcionalidades inicialmente no previstas en la fase de definición de los requerimientos del sistema. Algunas de estas nuevas funcionalidades se han integrado en el sistema y otras se han incluido en su roadmap, entre las cuales se destacan las siguientes:

- Mejorar la seguridad del segmento de cuarentena implantando una política de cuarentena que prohíba la comunicación a nivel dos (capa de enlace) entre los ordenadores conflictivos. Aunque se trate de una funcionalidad actualmente no estandarizada, los principales fabricantes de networking la implementan.
- Integración con la base de datos de información de red (inventario de ordenadores y conmutadores, usuarios, direcciones de red, tomas de datos, etc.) en proceso de desarrollo.
- Integración con el sistema de gestión de incidencias en proceso de desarrollo.
- Desarrollo de un módulo para que agentes externos puedan informar automáticamente al sistema de nuevos dispositivos conflictivos detectados.
- Análisis de la posible integración del sistema en el software de gestión open source Cacti[14] a través de un plugin.

El sistema final desarrollado goza de una gran flexibilidad

En el momento de la redacción de estas líneas se está organizando el primer piloto de implantación del sistema. Para evaluar el correcto funcionamiento del sistema, y antes de implantarlo en la red de la universidad, se ha elegido un escenario especial en el cual sus actores (de los diferentes perfiles: operador de seguridad, operador de helpdesk y usuario final) realizarán un uso intensivo del sistema y podrán transmitir fácilmente su feedback a los desarrolladores e integradores. El sistema se implantará en el segmento, o VLAN, dedicado a nuevos ordenadores y usado por el servicio de helpdesk de la universidad para completar las instalaciones y configuraciones sobre ellos. La flexibilidad del sistema desarrollado permite su uso tanto para la gestión de un segmento de cuarentena como de un segmento "incubadora" en la cual sus ocupantes no están aún preparados para acceder a la red de forma segura.

Anteriormente a este piloto se ha realizado otro proyecto piloto que únicamente pretendía verificar el correcto funcionamiento del binomio de funcionalidades, autenticación MAC y asignación dinámica de VLAN vía RADIUS, en la electrónica de red de acceso implantada en la universidad. De esta forma, se prevé que los resultados del proyecto piloto sean buenos ya que el binomio tecnológico en que se basa, que depende de la habilidad del fabricante de red, funciona correctamente.

Una funcionalidad es mejorar la seguridad del segmento de cuarentena implantando una política de cuarentena que prohíba la comunicación a nivel 2 entre ordenadores conflictivos

El servicio de red desarrollado y descrito en este artículo es un claro ejemplo de cómo la tecnología puede mejorar la calidad de un servicio institucional como es el caso del helpdesk y, al mismo tiempo, reducir considerablemente el esfuerzo y la dedicación necesarios para ello. Es más, sin un servicio mecanizado de gestión de ordenadores conflictivos como el propuesto, en la mayoría de los casos se cierran los ojos y se tratan sólo las incidencias más graves ya que se desbordaría por completo el servicio de microinformática. Los lazaretos que actualmente siguen en pie se dedican a otros usos ya que hace muchos años que desapareció la problemática. En el caso de la telemática, actualmente no se prevé a corto o medio plazo la desaparición de tal problemática y, por tanto, sería de gran utilidad que este nuevo servicio pasara a formar parte del catálogo de servicios de una red de ordenadores.

Referencias

[1] *"El Lazareto de Mahón, una fortaleza sanitaria"*. Josep M. Vidal Hernández. IME, 2002.

[2] *"Remote Authentication Dial In User Service (RADIUS)"* RFC 2865. Rigney, C., Willens, S., Rubens, A., Simpson,W., 2000.

[3] *"IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines"* RFC 3580. Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J., 2003.

[4] " *RADIUS Attributes for Tunnel Protocol Support"* RFC 2868. Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., Goyret, I., 2000.

[5] The FreeRADIUS Project. *http://www.freeradius.org*

[6] MySQL. Sun Microsystems. *http://www.mysql.com*

[7] Apache Web Server. The Apache Software Foundation. *http://www.apache.org*

[8] PHP. *http://www.php.net/*

[9] Iptables. Netfilter.org project. *http://www.netfilter.org*

[10] DHCP server (dhcpd). Internet Systems Consortium. *http://www.isc.org*

[11] Fake ARP daemon (farpd). Dug Song (dugsong@monkey.org) y Niels Provos (provos@citi.umich.edu).

[12] Postfix. *http://www.postfix.org*

[13] Nessus. Tenable Network Security. *http://www.nessus.org*

[14] Cacti. *http://www.cacti.net*

[15] *"Estudio de la aplicación del binomio IEEE 802.1X-EAP en el control de acceso a una red de área local basada en el estándar IEEE 802.3"*. Miquel Bordoy y Antonio Sola. Actas del I Simposio sobre Seguridad Informática [SSI'2005]. Thomson Paraninfo (ISBN: 84-9732-447-1).

Miquel Bordoy
(miquel.bordoy@uib.es)
Ricardo Díaz
(ricardo.diaz@uib.es)
Antonio Sola
(toni.sola@uib.es)
Centre de Tecnologies de la Informació
Universitat de les Illes Balears