ALTAIR-SIGVI: UN NUEVO SISTEMA PARA COMBATIR EL CIBERCRIMEN MITIGANDO LAS VULNERABILIDADES

ALTAIR-SIGVI: MITIGATE VULNERABILITIES, A NEW WAY TO WORK AGAINST CYBERCRIME

Autor:

Víctor Huerta Cerezuela. Universidad Politécnica de Cataluña.victor.huerta@upc.edu

Resumen:

Uno de los retos a los que se enfrentan los administradores de sistemas informáticos hoy es el evitar que los recursos TIC que gestionan se usen para realizar ciberdelitos, o sufrir el impacto en sus propios servicios de ciberataques. En este artículo se explica el reto de poner en marcha un nuevo modelo operativo que permita incrementar la ciberseguridad de nuestras infraestructuras tecnológicas con la herramienta ALTAIR-SIGVI que nos alerta de las vulnerabilidades y nos permite auditar nuestros recursos y servicios informáticos.

Abstract:

Managing technological infrastructures has a new challenge. This challenge is to prevent the use of our computers to do cybercrimes or be affected by a cyberattack. In this article we explain a new way to implement a service to provide better security against new cybersecurity attacks. With the new tool ALTAIR-SIGVI, we can increase our security doing a better vulnerability management.

Palabras clave:

Seguridad, Vulnerabilidades, Auditoría.

Keywords:

Security, Vulnerabilities, Audit.

1. ¿A QUÉ NOS ESTAMOS ENFRENTANDO?

Cuando hoy en día hablamos de ciberseguridad y no de seguridad informática es porque lo que hace dos décadas nos preocupaba eran los hackers y hoy lo que nos preocupa son los delincuentes cibernéticos. Además, esas preocupaciones también han madurado, la cultura del hacker que conocimos y que sigue existiendo, es una cultura que nos iluminaba sobre las vulnerabilidades de nuestros recursos tecnológicos. Aunque muchas veces esas "iluminaciones" fueran a base de tragarnos nuestro orgullo y de muchas horas de reinstalar y securizar equipos. Ahora nuestra preocupación sobre las vulnerabilidades ha madurado hacia el uso que se puede hacer de ellas para cometer delitos penados por la ley, como puede ser el robo de información, la estafa o la incapacitación de proveer un servicio.

1.1. El cambio del perfil del atacante

Aunque la figura del hacker sigue existiendo, hoy en día el perfil del atacante se asemeja más al de un delincuente. Básicamente porque ya no hace falta ser un gran experto en tecnologías informáticas o de telecomunicaciones para poder realizar un ataque informático, y/o porque el objetivo que se busca es más una recompensa económica o una satisfacción por hacer daño a un enemigo.

En Febrero de este año, las portadas de algunos diarios digitales se hacían eco de que una niña británica de siete años "aficionada a la tecnología" logró hackear una red wifi[1]. ¿Cómo lo logró? viendo un video tutorial en Youtube de cómo hacerlo.

Pero este no es el perfil que nos debe preocupar. Este caso, lo que refleja es que la información que hoy en día podemos encontrar en Internet poniendo en el buscador google la frase "como hackear una wifi" da más de medio millón de resultados. A partir de este punto, podríamos ir a un segundo nivel y obtener información de lo que circula por esa red. De ahí a poder robar información relativa a tarjetas de crédito

[1] http://www.europapress.es/portaltic/internet/noticia-nina-siete-anos-capaz-hackear-red-wifi-10-minutos-20150218173709.html

hay un pequeño paso, que nos puede llevar a la venta de esa información a organizaciones criminales[2].

Hoy en día podemos hablar de tres perfiles diferentes. El cibercriminal que tiene como objetivo el robo de datos o la extorsión. Son personas que buscan un beneficio económico, por ejemplo, en la venta de datos robados de tarjetas de crédito o en el robo de identidades digitales. Que extorsiona a empresas o personas pidiendo dinero a cambio de hacerles visibles sus datos encriptados mediante un virus (*ransomware*[3]) o mediante la amenaza de realizar acciones dañinas contra sus servicios web (*DDoS*[4] Ataques de Denegación de Servicio Distribuido). El segundo perfil de atacante sería el del cibercriminal que busca información de competidores o enemigos con el objetivo de efectuar acciones de espionaje industrial o el sabotaje de servicios de la competencia. El tercer y último perfil del atacante es aquel que comúnmente llamamos hacktivista y que tiene como objetivo principal el efectuar acciones públicas de protesta mediante el ataque y puesta en evidencia de gobiernos o grandes compañías. Existen otros dos tipos de atacantes en la red que por su complejidad no abordaremos en este artículo, hablamos de los terroristas que usan la red Internet para cometer acciones de publicidad o robo de identidades u obtención de dinero, y por último el presunto uso que hacen algunas agencias gubernamentales de las técnicas de los atacantes descritos anteriormente para enfrentarse a países u organizaciones no amigas.

1.2. Los nuevos ciberdelitos

Igual que en estos últimos años han cambiado quienes nos atacan en la red, también han cambiado los delitos. Si nos fijamos en la siguiente tabla[5] de los delitos informáticos más importantes a lo largo del año 2014 en Estados Unidos, podremos apreciar dos cosas, el gran volumen de información robada y el tipo de información que se quiere robar.

[2]http://www.bbc.co.uk/mundo/noticias/2014/11/141110_tecnologia_crimen_organizado_cibercrimen_tarjetas_credito_ig
[3] http://es.wikipedia.org/wiki/Ransomware
[4] http://es.wikipedia.org/wiki/Ataque_de_denegación_de_servicio
[5] http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect

Fecha (2014)	Empresa	Cantidad de datos expuestos	Tipo de dato
25 enero	Michael's	2.600.000	payment cards
6 febrero	Home Depot	20.000	employee info
14 marzo	Sally Beauty Supply	25.000	credit/debit card
17-abr	Aaron Brothers	400.000	payment cards
22-abr	Iowa State University	48.729	student social security numbers
30 mayo	Home Depot	30.000	credit/debit card
22-jul	Goodwill Industries	868.000	payment systems
18 agosto	Community Health Systems	4.500.000	patient data
21 agosto	United Postal Service	105.000	credit/debit card
28 agosto	JP Morgan Chase	1.000.000	financial information
2 septiembre	Home Depot	56.000.000	credit/debit card
2 septiembre	Viator/Trip Advisor	880.000	payment cards
25 septiembre	Central Dermatology	76.258	patient data
7 noviembre	Home Depot	53.000.000	email addresses
10 noviembre	US Postal Service	800.000	personal data
18 noviembre	Staples	1.200.000	credit/debit card

http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect

Está claro que uno de los nuevos delitos que están surgiendo con fuerza en internet es el del delito financiero.

Evidentemente existen otros delitos en la red como pueden ser los mal llamados inocuos como el spam (correo electrónico no solicitado), u otros delitos más relevantes e impactantes como pueden ser el fraude informático, el hostigamiento o acoso, llegando al tráfico de drogas o el terrorismo virtual. Y nunca se ha de bajar la guardia con los delincuentes sexuales, que han encontrado en Internet una forma más ágil de ocultar su identidad y poder delinquir haciendo grooming[6] .

1.3. La dimensión exponencial de dispositivos

Si a los nuevos perfiles de atacantes y al conjunto de tipos de delitos que se están cometiendo por la red, añadimos el crecimiento exponencial de los dispositivos conectados, tenemos un campo de cultivo extremadamente fértil para la ciberdelincuencia.

[6] Una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él. http://es.wikipedia.org/wiki/Grooming

La Internet de las cosas (IoT – Internet of Things) es el nuevo concepto que se está aplicando para poder hablar de cuándo habrá más equipos conectados a Internet que personas. Todos somos conscientes que a fecha de hoy no tan sólo están conectados a Internet equipos domésticos como la televisión, el DVD, el tablet, etc., sino también podemos encontrar desde neveras, encimeras y hasta macetas que te indican el nivel de humedad de la tierra. Esto no es nada, ya que cuando salimos de casa, desconocemos la cantidad de sensores de temperatura, sensores de movimiento, cámaras de videovigilancia, etc., que también están conectadas a Internet. Si a todo esto le sumamos, la cantidad de equipos que encontramos en nuestro trabajo y que también están conectados a la red, desde el ordenador de trabajo, pasando por la impresora, y llegando a dispositivos mucho más específicos como podría ser en el ámbito de la salud: productos de consumo para la vigilancia de la salud (ejemplo: pulseras de monitorización), dispositivos médicos externos portátiles (ejemplo: bombas de insulina portátiles), dispositivos médicos incrustados internamente (ejemplo: marcapasos), y dispositivos médicos estacionarios pero conectados en red (ejemplo: monitorización cardiaca).

Si habláramos ahora de ejemplos en ámbitos como la infraestructura urbana con el auge de las smartcities[7], el uso de sensores para la monitorización del control medioambiental, el auge de los dispositivos de control de producción y gestión de calidad en las industrias mecánicas, alimentarias, etc… nos encontraríamos con unas cifras escalofriantes de equipos conectados a la red.

¿Dónde está el peligro?, en que con tanta masificación nos olvidamos muchas veces de controlar la vulnerabilidad de esos dispositivos, muchos de los cuales ni vemos, ni sabemos que los tenemos, y hasta nos olvidamos de actualizar o simplemente nos olvidamos de comprobar su seguridad antes de conectarlos a la red (ejemplo: “No pases el repositorio de código a producción en tu dispositivo… o atente a las consecuencias” por Amador Aparicio[8]).

[7] http://es.wikipedia.org/wiki/Ciudad_inteligente
[8] http://www.elladodelmal.com/2014/11/no-pases-el-repositorio-de-codigo.html

2. COMO COMBATIR EL CIBERCRIMEN MITIGANDO LAS VULNERABILIDADES

Una de las medidas principales que nos ha de permitir combatir el cibercrimen, es la de evitar al máximo de lo que nos sea posible, el que esos millares de dispositivos que están conectados a Internet sean vulnerables a ataques de ciberdelincuentes.

2.1. Que entendemos por vulnerabilidades

Las vulnerabilidades son aquellas debilidades de nuestro sistema informático que permiten que una amenaza pueda producir un daño (material o inmaterial) sobre los elementos de nuestro sistema. Este daño puede violar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones que gestionamos. También existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanas, así como las amenazas de origen interno, como la negligencia del propio personal.

En este artículo nos vamos a centrar en las vulnerabilidades provocadas por amenazas de tipo tecnológico comúnmente definidas como bugs de seguridad. Estos errores de software, hardware o firmware provocan normalmente un funcionamiento anómalo del equipo informático que los aloja, permitiendo o bien un uso no autorizado del mismo, o hasta la desconexión operativa del propio equipo.

2.2. Los avisos de vulnerabilidades

Al igual que algunas de las violaciones de datos bancarios del año 2014 descritas anteriormente, otras vulnerabilidades, igual de preocupantes, se dieron a conocer durante el año pasado, haciéndonos pensar si realmente el uso de Internet empezaba a ser peligroso.

De los cientos de avisos de vulnerabilidades recibidos el año pasado, uno de los más impactantes fue sin duda el Heartbleed/OpenSSL. Mediante un agujero de seguridad en la implementación de los protocolos de seguridad de la capa de transporte de OpenSSL, se podía llegar a desencriptar información que circulaba por Internet. La noticia de este error se extendió muy rápidamente, y dejó millones de sitios web expuestos a lo que se pensaba que era una comunicación segura, ya que

la mayoría de equipos informáticos conectados a Internet usan por ejemplo Apache con Open SSL como servidor web.

Otra vez nos encontramos con la conjunción de un número inimaginable de dispositivos conectados, una misma vulnerabilidad, y un canal de difusión extremadamente rápido como pueden ser las redes sociales, lo que nos lleva a un caldo de cultivo perfecto para que los nuevos ciberdelincuentes encuentren formas ágiles y rápidas de realizar sus ataques.

Como parece que es imposible estar completamente seguros que nuestros equipos informáticos estén libres de vulnerabilidades y por lo tanto que estemos nosotros libres de ser atacados, lo que hay que hacer es trabajar para estar lo mejor y más rápidamente informados de estas vulnerabilidades para poder arreglar esos errores y mitigar posibles ataques.

2.3. La gestión de las vulnerabilidades versus nuestro propio modelo organizativo

Para poder exponer cómo combatir el cibercrimen mediante los avisos de vulnerabilidades, he tomado como ejemplo mi propio entorno de trabajo. Las acciones que estamos desarrollando en nuestra universidad no están encaminadas a erradicar por completo el uso delictivo de nuestros equipos, eso sería una tarea imposible por dos motivos: la seguridad informática plena no existe, y el uso de recursos económicos para llegar a unos niveles máximos serían desproporcionados teniendo en cuenta el momento de crisis por el que estamos pasando en todo el sistema universitario español.

Dicho esto, no nos hemos de cruzar de brazos, y se han de buscar soluciones que se adapten a nuestro entorno organizativo, que sean ágiles de poner en explotación, y que aunque incrementen inicialmente la dedicación del personal, a la larga reduzcan las horas de atención.

En nuestra universidad nos encontramos con más de 22 escuelas o facultades, 42 departamentos y 10 institutos de investigación, repartidos en 7 ciudades. Este número de unidades y dispersión geográfica hace que la gestión de la informática y las telecomunicaciones se haga de forma centralizada para lo que son servicios más generales o institucionales, y descentralizada para lo que son servicios más específicos o más próximos al estudiante, profesor o personal de administración y servicios.

Para que se hagan una idea, en mi caso, como Responsable de Seguridad TIC, colaboro con unas 50 unidades que gestionan sus propios equipos informáticos o sus propios servicios de información.

De estas 50 unidades, hay algunas que tienen por su importancia o volumen de usuarios, personal dedicado parcialmente a temas de seguridad informática, pero en la mayoría, nos encontramos con técnicos que deben, entre otras muchas tareas controlar un importante volumen de hardware y software de docencia, investigación y desarrollo, buscando la colaboración de los investigadores que configuran o trabajan con esos equipos.

A lo largo de los últimos 10 años, hemos trabajado con un modelo que se ha demostrado poco operativo. Se basaba en el registro voluntario de estos profesionales informáticos en una lista de distribución donde se recibían los avisos de vulnerabilidades detectados por Equipos de Respuesta ante Emergencias Informáticas (CERT[9]), también los avisos publicados por el NIST[10], y los boletines de seguridad de fabricantes de hardware y software, utilizando un formato estándar que es el Common Vulnerabilities and Exposures (CVE[11]).

[9] http://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Informaticas
[10] https://web.nvd.nist.gov/view/vuln/search
[11] http://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Una de las bases de datos de vulnerabilidades disponible en España es la que ofrece INCIBE [12] (Instituto nacional de Ciberseguridad) mediante su CERT con un repositorio de más de 65.000 registros de información traducida al español. Tal como indican en su web, cada una de las vulnerabilidades enlaza a diversas fuentes de información así como a distintos parches o soluciones. También permiten la búsqueda de información mediante la selección de criterios de tipo de vulnerabilidad, fabricante, impacto, etc… además de permitir la suscripción a esta base de datos mediante tecnología RSS[13].

¿Porque no llegó a ser operativo el que el personal TIC de la universidad recibiera estos avisos de vulnerabilidades? En primer lugar porque se llegaban a recibir en algunos días concretos más de 50 correos electrónicos donde por cada una de las posibles versiones de un mismo software nos podía llegar el mismo tipo de aviso de vulnerabilidad. En segundo lugar, hasta la llegada hace un año del servicio anteriormente descrito de INCIBE, los mensajes no llegaban en castellano, dificultando su comprensión. En tercer lugar, una vulnerabilidad para ser incorporada al proceso de aviso debe pasar por unas etapas de validación, por lo que se hace imposible el obtener vulnerabilidades de 0-day (ataques de día cero). Estas vulnerabilidades de día cero son las más peligros y dañinas ya que se expanden con rapidez por las redes aprovechando el desconocimiento sobre cómo resolverlas y que parche o solución aplicar.

Evidentemente, cuando de un volumen ingente de información tienes que empezar a hacer una selección de una información que no viene en un idioma cómodo para un técnico, o cuando estos avisos no pueden incorporar las vulnerabilidades de mayor impacto, al final se impone el hacer caso omiso, y no gestionar los avisos de vulnerabilidad.

[12] https://www.incibe.es
[13] http://es.wikipedia.org/wiki/RSS

2.4. El modelo funcional ALTAIR-SIGVI

Hace algunos años se inició un desarrollo propio en nuestra universidad, la herramienta SIGVI (Sistema Inteligente de Gestión de Vulnerabilidades Informáticas). Se planteó entonces que la herramienta fuera de código abierto y que diera solución a la necesidad de automatizar las tareas de recolección, comparación y aviso de vulnerabilidades. Además, se quería proporcionar a los administradores de sistemas un entorno colaborativo de seguimiento de las alertas, así como un repositorio de vulnerabilidades. Proporcionando a la vez a los responsables un entorno de consulta del estado de las infraestructuras y la posibilidad de emitir informes.

Esta herramienta ha ido evolucionando a lo largo de estos años, gracias a los desarrollos realizados por el personal TIC de UPCnet[14], y del inLab FIB esCERT[15], hasta llegar a lo que hoy denominamos ALTAIR-SIGVI.

Este modelo de desarrollo nos garantiza una evolución permanente de la herramienta, adaptándola nuevos requisitos externos, así como a posibles cambios del modelo organizativo de la gestión de las TIC de la universidad.

El diseño de esta herramienta se ha basado en los siguientes requisitos funcionales: accesibilidad web, compendio de diferentes protocolos de gestión de vulnerabilidades (CVE, CPE[16], CVSS[17], etc…), descubrimiento de activos automático, gestión de alertas, sistema de escaneo de vulnerabilidades, sistema de monitorización, servicios informativos y gestión de tareas rutinarias.

Así mismo, se han trabajado requisitos no funcionales como usabilidad, estabilidad, seguridad, escalabilidad, documentación y licencia open source.

[14] http://www.upcnet.es/es
[15] http://inlab.fib.upc.edu/es/entitats/escert
[16] Common Platform Enumeration. https://cpe.mitre.org/about
[17] Common Vulnerability Scoring System. https://www.first.org/cvss

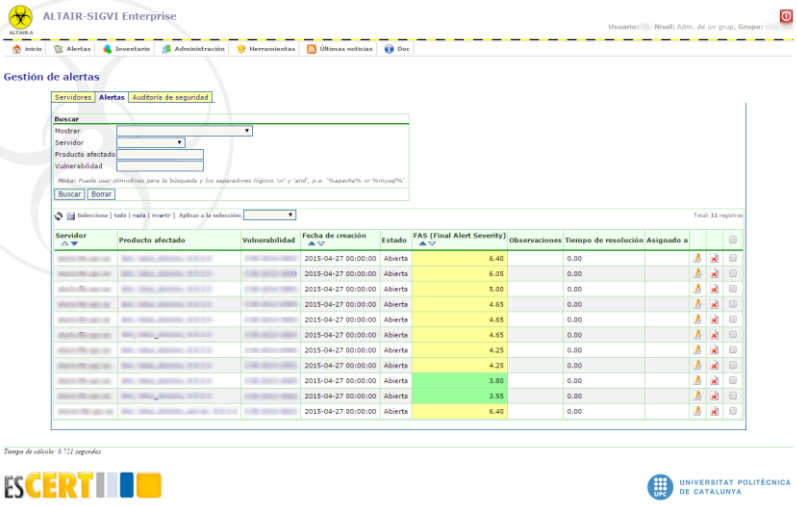
El producto ALTAIR-SIGVI integra NSDi [18](Network Services Discoverer) para el descubrimiento de activos en nuestra red y servicios visibles desde fuera mediante tecnología Nmap[19] y OpenVAS[20].

2.5. En que consiste la herramienta ALTAIR-SIGVI

La herramienta ALTAIR-SIGVI es la integración de un conjunto de servicios y herramientas de libre distribución que permite ofrecer a los administradores de sistemas un entorno de gestión de las vulnerabilidades en la infraestructura tecnológica bajo su responsabilidad.

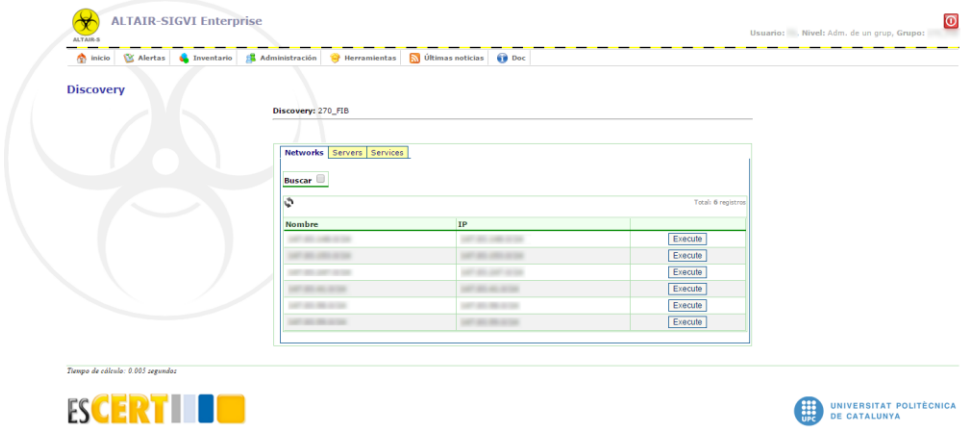
ALTAIR-SIGVI integra:

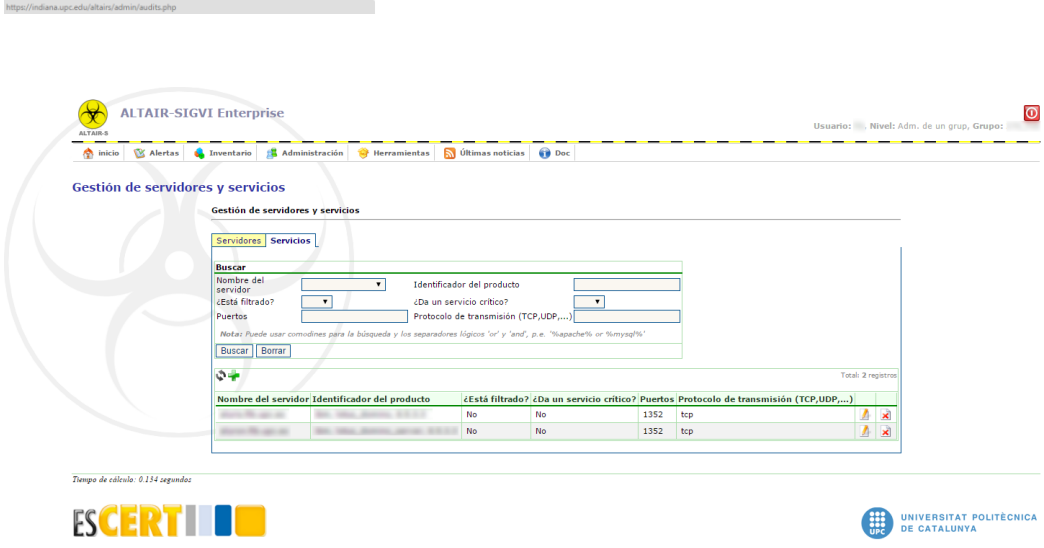
- Una base de datos de avisos de vulnerabilidades que permite conocer en profundidad el impacto que pueden tener, acceder a las medidas a tomar para mitigar el impacto, y referencias del fabricante o desarrollador del producto afectado.



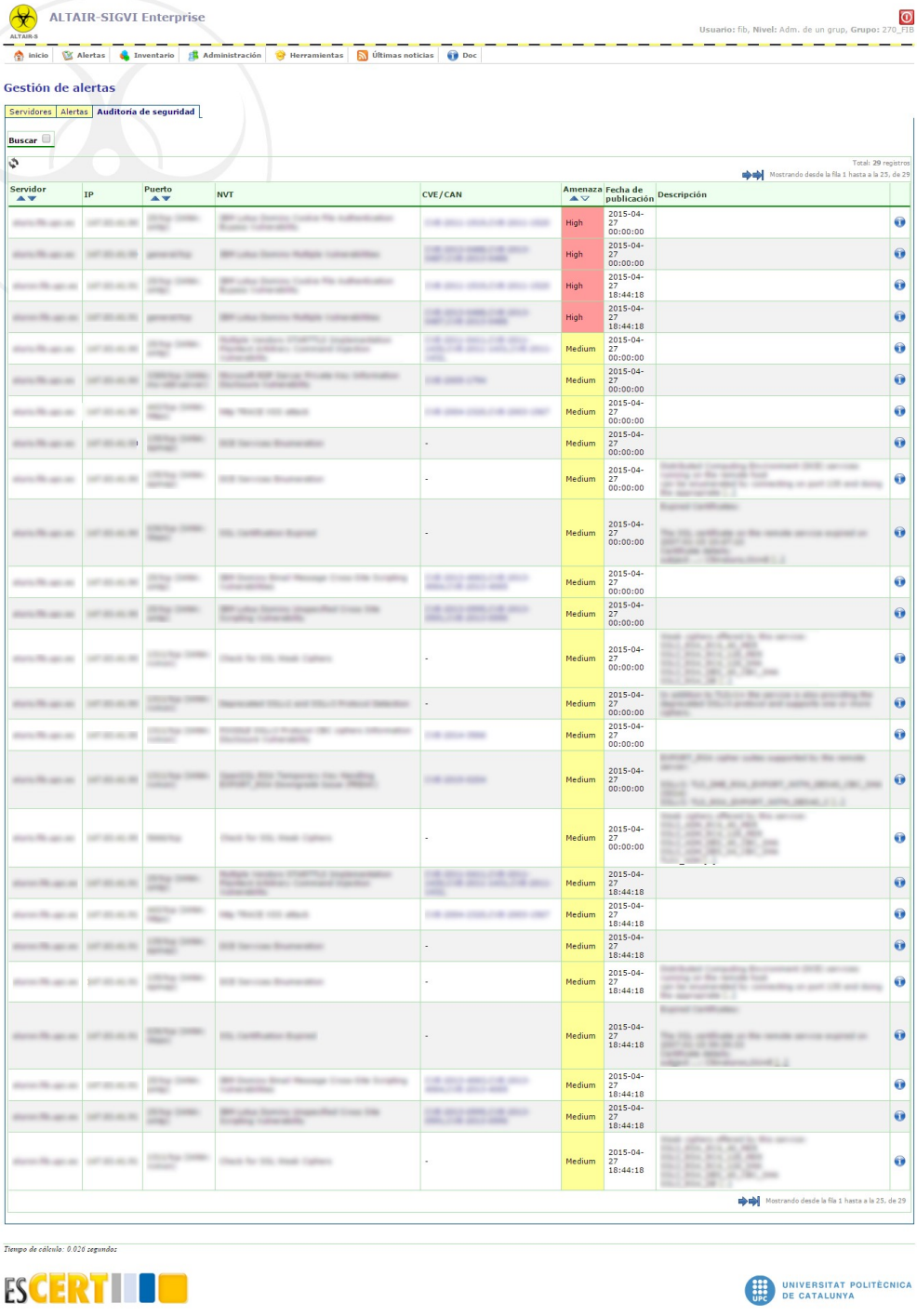
[18] http://nsdi.sourceforge.net
[19] https://nmap.org
[20] Open Vulnerability Assessment System. http://www.openvas.org

- Una herramienta para la detección automática de equipos y servicios conectados en nuestra red. La posibilidad de incorporar estos elementos a una base de datos para inventariarlos, incluyendo las versiones de software y hardware de cada uno de ellos. El uso de metadatos y métricas estandarizadas para la catalogación de equipos y servicios según su nivel de criticidad.

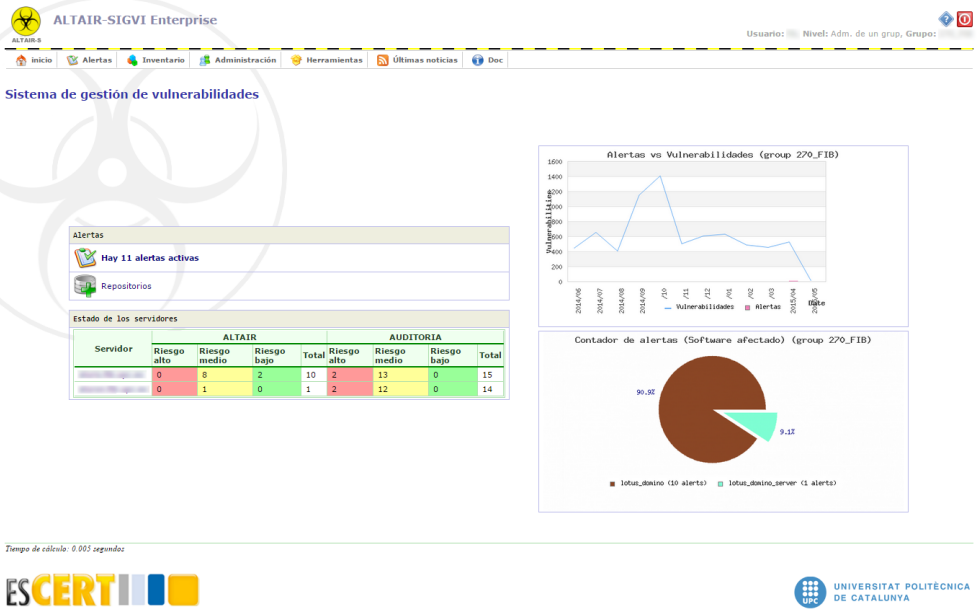




- Un escáner de vulnerabilidades que mediante la exploración de nuestra red (puertos, aplicaciones web, y acceso a bases de datos), y mediante esta auditoría de seguridad, determina cuales de las vulnerabilidades registradas afectan a nuestro inventario de equipos.



- Un panel informativo que permite determinar las alertas activas y su grado de importancia.



En definitiva ALTAIR-SIGVI permite saber qué servicios de nuestra red están al descubierto, es decir, que son accesibles desde fuera mediante el escaneo para detectar qué IPs y puertos están abiertos y qué servicios ofrecen, y si estos son vulnerables.

3. UNA NUEVA MANERA DE IMPLANTAR UN SERVICIO DE GESTIÓN DE VULNERABILIDADES

3.1. Un nuevo modelo de implantación del servicio ALTAIR-SIGVI

Como ya hemos dicho anteriormente llevamos ya algunos años intentando ofrecer herramientas que ayuden a los administradores de sistemas a incrementar la seguridad de las infraestructuras que gestionan.

Alguna de estas iniciativas no han tenido éxito, ya sea por el volumen de datos a procesar, ya sea por la complejidad de nuestros propios modelos organizativos que dificultan algunas veces un correcto dimensionamiento o una correcta eficacia de los modelos funcionales puestos en explotación.

Ahora que teníamos una nueva y potente herramienta en nuestras manos, debíamos apostar por estudiar cómo mejorar el modelo de implantación de este nuevo servicio. Para poder garantizar el éxito de este nuevo servicio, lo primero que se determinó es que su éxito podía pasar por darlo de baja si no superaba un proceso de evaluación. A veces hay que empezar un proyecto teniendo claro que se ha de evaluar una vez puesto en marcha y dándole un margen de funcionamiento concreto para asentarse y determinar si realmente se usa y si el coste de mantenerlo en activo es asumible por la organización.

Partiendo de esta premisa, se trabajó la fase de implantación del servicio teniendo en cuenta los siguientes ejes operativos:

- El producto ha de estar instalado en un servicio en la nube que garantice su escalabilidad, capacidad, fiabilidad y seguridad.
- Se ha de trabajar con los factores y elementos relativos a la experiencia de usuario para poder no sólo depender de factores relativos al diseño del producto sino además de aspectos relativos a las emociones, sentimientos, y en la confiabilidad del producto
- La definición de unos SLA's (acuerdos de niveles de servicio) que determine su funcionamiento y permita evaluar su calidad.
- El servicio de gestión de vulnerabilidades ha de tener un soporte por parte de personal especializado.
- ALTAIR-SIGVI es una herramienta basada en software libre que requiere de un servicio de mantenimiento que garantice su actualización.
- La impartición de un módulo formativo avanzado para sus usuarios que permita mejorar la experiencia de usuario.

Llegaba entonces el momento de diseñar el modelo de implantación. Una primera fase del proyecto de puesta en explotación del servicio se inició con la recogida de indicadores actuales sobre la gestión de las vulnerabilidades.

Esta definición de indicadores, y su posterior recolección, nos permiten tener una fotografía exacta de la situación actual. Hay que recordar que nuestro objetivo es poder determinar al finalizar el periodo del margen de confianza dado, si los costes de mantener ALTAIR-SIGVI como servicio son asumibles por nuestra universidad.

Los tipos de indicadores que se han definido incluyen los más técnicos como por ejemplo número de vulnerabilidades gestionadas, número de denuncias recibidas, número de avisos de entornos desprotegidos recibidos, volumen de máquinas donde se gestiona la seguridad de forma activa, etc.

Pero también se incluyen indicadores sobre los recursos humanos dedicados actualmente a temas de seguridad como por ejemplo: horas del personal dedicadas a atender vulnerabilidades, horas del personal dedicadas a resolver el impacto de ataques, etc.

Sin olvidarnos de los indicadores más importantes que son los relativos a la experiencia de usuario. Estos indicadores inicialmente sólo pueden reconocer la parte cualitativa del sistema actual indicando su grado de satisfacción sobre la gestión de las vulnerabilidades incluyendo datos de satisfacción por ejemplo sobre el soporte que se recibe.

Las siguientes fases son:

- ***Fase de prueba de concepto*:** Se buscaron 5 unidades de las 50 descritas anteriormente para realizar una implementación del servicio ALTAIR-SIGVI de forma resumida con el propósito de verificar que el servicio es susceptible de ser explotado tal como se definió. En esta fase se acabaron de pulir los indicadores elegidos para evaluar el servicio, se trabajó de manera más directa con el usuario final para poder observar sus reacciones en el uso de todos los componentes del

servicio, y sobretodo, se trabajó en mediar las reacciones sobre la confiabilidad del producto. El objetivo de esta fase incluía el poder determinar si los usuarios se volvían "alérgicos" o "adictos" a ALTAIR-SIGVI, para poder determinar la continuidad o no del proyecto, y en caso afirmativo conseguir que estas 5 unidades actuasen de forma activa en la siguiente fase.

- ***Fase de divulgación*:** Esta fase consiste en que el propio usuario final, en ese caso las 5 unidades de la fase de prueba de concepto, divulgase la necesidad de implantar este nuevo servicio al resto de profesionales TIC de la universidad implicados en temas de administración de equipos o gestión de sistemas de información. Esto se haría mediante la organización de una jornada donde inicialmente ponentes externos introdujeran los conceptos actuales y ejemplificados de los efectos que tienen las vulnerabilidades en los ataques cibernéticos que estamos sufriendo. A partir de ahí, los propios informáticos de la universidad que ya han cogido una experiencia favorable con ALTAIR-SIGVI presentarían el nuevo servicio a sus compañeros, hablándoles de tú a tú ya que conviven con las idénticas situaciones laborales (falta de recursos técnicos y humamos, incremento de dispositivos, incremento de la autoconfiguración por parte de los usuarios finales, etc…).

- ***Fase de explotación inicial*:** Esta fase sería la típica fase donde se pone en marcha el servicio haciendo un seguimiento inicial y adaptando los recursos de la nube a la demanda por parte de los usuarios. Con el objetivo de innovar en la puesta en marcha del servicio de gestión de vulnerabilidades, se ha incorporado a esta fase un módulo formativo de seis horas para los técnicos que decidan usar ALTAIR-SIGVI.

  Este módulo formativo se ofrece una vez se garantice que los usuarios han utilizado la herramienta ALTAIR-SIGVI durante dos meses. Lo que se pretende es profundizar sobre los conocimientos de la herramienta, compartir casos de uso reales y presentar técnicas complementarias que permitan tener una fotografía periódica del estado de seguridad de nuestras redes mediante auditorías.

Como resultado de la acción formativa, la persona participante podrá: Llevar a cabo un descubrimiento de software mediante la herramienta; Dar de alta automáticamente nuevos activos en ALTAIR-SIGVI; Gestionar el nivel de riesgo de una red en todo momento; Entender los procesos de auditorías de seguridad; Realizar auditorías internas para conocer el estado de la seguridad de una red.

- Y por último queda la **fase final** que denominamos *Fase de evaluación* y que describimos en los siguientes apartados.

3.2. La evaluación continuada de indicadores

Como ya hemos descrito anteriormente, en una primera fase se definen un grupo de indicadores que nos han de permitir al cabo de unos meses determinar si el uso de ALTAIR-SIGVI es el adecuado para los recursos que se necesitan para mantenerlo.
Esta evaluación implica la participación de todos los usuarios, ya que han de ser ellos los que finalmente juzguen la necesidad del servicio de gestión de vulnerabilidades tal como se ha definido ya que han participado de forma activa en su desarrollo. En definitiva, los profesionales TIC de la universidad, encargados de gestionar la seguridad de los equipos e infraestructuras TIC de sus unidades, han de ser capaces de poder evaluar mediante los indicadores descritos anteriormente si el diseño de este servicio es el adecuado, si las expectativas generadas son correspondidas, si los recursos asignados para el soporte y mantenimiento son los adecuados, etc.

Existirá pues, un primer proceso de autoevaluación donde se reunirá a todos los usuarios para exponerles los resultados de los indicadores recogidos, donde se hablará con los desarrolladores de ALTAIR-SIGVI, donde estarán las personas que dan soporte y lo mantienen, y entre todos se definirá la madurez del servicio así como su grado de confiabilidad.

Si el resultado de esta evaluación principal es positivo, se definirán las métricas que se seguirán a partir de ahora para evaluar los indicadores de uso y satisfacción y la periodicidad de las siguientes evaluaciones.

Estas evaluaciones continuadas han de permitir determinar la calidad de la herramienta en relación a las actualizaciones que se tengan que realizar, así como a los mantenimientos evolutivos que requiere por la mejora de la tecnología o la incorporación de nuevos servicios.

3.3. La obligación de transferir el conocimiento y nuestra experiencia

Si de todos los procesos anteriormente descritos se obtiene como resultado un servicio satisfactorio, deberemos asumir el reto de poner esta "buena práctica" a disposición del sistema universitario español.

Las universidades públicas somos generadoras de conocimiento y buenas prácticas, y tenemos la obligación de transferir este conocimiento al sector para contribuir al desarrollo del país.

Es por este motivo, que el diseño de este nuevo servicio de gestión de vulnerabilidades, ALTAIR-SIGVI ha incorporado mecanismos que hagan factible su aprovechamiento como software libre mediante una licencia GNU General Public License (GPL). Este tipo de licencia permite la libre distribución, modificación y uso del software, pero con la obligación de mantener esta libertad, no pudiendo ser modificado para construir software propietario.

Además, se ha trabajado desde el inicio con la voluntad de poder ofrecer a quien esté interesado, ALTAIR-SIGVI como Software as a Service[21] (SaaS). Aprovechando el modelo organizativo de nuestra universidad, donde sus servicios informáticos centralizados son ofrecidos por UPCnet, una empresa de consultoría y servicios TI de la propia universidad y donde podemos contar con el inLab FIB como laboratorio de innovación e investigación de la Facultad de Informática de Barcelona de la Universitat Politècnica de Catalunya - Barcelona Tech (UPC) que integra profesorado de diferentes departamentos de la UPC y su propio personal técnico para ofrecer soluciones en diferentes áreas.

[21] http://es.wikipedia.org/wiki/Software_como_servicio

4. CONCLUSIONES

La protección de los activos de las diferentes redes de una organización precisa de herramientas que ayuden a tener información detallada y actualizada de los diferentes elementos implantados.

La gestión del inventariado y el conocimiento de las vulnerabilidades que pueden afectar a nuestros equipos o servicios, permiten minimizar los riesgos al aplicar las medidas de contención necesarias.

Ponemos a disposición del personal del ámbito TIC el servicio ALTAIR-SIGVI, una herramienta de gestión de la seguridad de activos que permite informarse de nuevas vulnerabilidades y auditar el nivel de seguridad de nuestros equipos o servicios en red.

El uso del servicio ALTAIR-SIGVI como integración de diferentes herramientas opensource de seguridad ayuda a minimizar el número de amenazas, como disminuye la dedicación de recursos relacionados con la gestión de prevención o gestión de incidentes de seguridad, garantizando su soporte y evolución.

El basar la continuidad del servicio en el uso por parte de los usuarios, la evolución positiva de los indicadores, y la evaluación continuada de la experiencia de usuario, nos ha de permitir tener no tan solo un servicio de calidad, sino también garantizar un servicio sostenible en el tiempo.

5. RECURSOS

- APARICIO, Amador. *No pases el repositorio de código de producción en tu dispositivo o atente a las consecuencias.* Un informático en el lado del mal. [Fecha de consulta: 30/04/2015]. Disponible en http://www.elladodelmal.com/2014/11/no-pases-el-repositorio-de-codigo.html

- *BBC.* [Fecha de consulta: 30/04/2015]. Disponible en http://www.bbc.co.uk/mundo/noticias/2014/11/141110_tecnologia_crimen_organizado_cibercrimen_tarjetas_credito_ig

- CPE. *Common Platform Enumeration.* [Fecha de consulta: 30/04/2015]. Disponible en https://cpe.mitre.org/about

- FIRST. *Common Vulnerability Scoring System.* [Fecha de consulta: 04/05/2015]. Disponible en https://www.first.org/cvss

- INCIBE. *Instituto Nacional de Seguridad*. [Fecha de consulta: 04/05/2015]. Disponible en https://www.incibe.es

- McLELLAN, Charles. *Cybersecurity in 2015: What to expect.* ZDNet. [Fecha de consulta: 04/05/2015]. Disponible en http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/

- NIST. *National Vulnerability Database.* [Fecha de consulta: 04/05/2015]. Disponible en https://web.nvd.nist.gov/view/vuln/search

- *Nmap.org.* [Fecha de consulta: 04/05/2015]. Disponible en https://nmap.org

- OpenVAS. *Open Vulnerability Assessment System.* [Fecha de consulta: 05/05/2015]. Disponible en http://www.openvas.org/

- *Portal TIC.* [Fecha de consulta: 05/05/2015]. Disponible en http://www.europapress.es/portaltic/internet/noticia-nina-siete-anos-capaz-hackear-red-wifi-10-minutos-20150218173709.html

- *Sourceforge.* [Fecha de consulta: 06/05/2015]. Disponible en http://nsdi.sourceforge.net

- UNIVERSITAT POLITECNICA DE CATALUNYA. *Escert.* [Fecha de consulta: 06/05/2015]. Disponible en http://inlab.fib.upc.edu/es/entitats/escert

- *UPCnet.* [Fecha de consulta: 06/05/2015]. Disponible en http://www.upcnet.es/es

- *Wikipedia. Ataque de denegación de servicio.* [Fecha de consulta: 06/05/2015]. Disponible en http://es.wikipedia.org/wiki/Ataque_de_denegación_de_servicio

- *Wikipedia. Ciudad inteligente.* [Fecha de consulta: 06/05/2015]. Disponible en http://es.wikipedia.org/wiki/Ciudad_inteligente

- *Wikipedia. Common vulnerabilities and exposures.* [Fecha de consulta: 07/05/2015]. Disponible en http://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

- *Wikipedia. Equipo de respuesta ante emergencias informáticas.* [Fecha de consulta: 07/05/2015]. Disponible en http://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Informaticas

- *Wikipedia. Grooming.* [Fecha de consulta: 04/05/2015]. Disponible en http://es.wikipedia.org/wiki/Grooming

- *Wikipedia. Ransonware.* [Fecha de consulta: 04/05/2015]. Disponible en http://es.wikipedia.org/wiki/Ransomware

- *Wikipedia. RSS.* [Fecha de consulta: 04/05/2015]. Disponible en http://es.wikipedia.org/wiki/RSS

- *Wikipedia. Software como servicio.* [Fecha de consulta: 04/05/2015]. Disponible en http://es.wikipedia.org/wiki/Software_como_servicio