GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

SECURING AN ISP, WHERE DO I START?
A Case Study

Author: Miguel Arévalo

GSEC Practical Assignment v1.4b Option 2
August 10, 2004

© SANS Institute 2004, Author retains full rights.

ÍNDICE

ÍNDICE **2**
1 ABSTRACT **3**
2 ¿CÓMO COMENZÓ LA SEGURIDAD EN EL ISP? **4**
3 MEJORANDO LA SEGURIDAD DEL ISP **7**
3.1 Recurso Humano 7
3.2 DNS 8
3.3 Acceso Físico 12
3.4 SERVIDORES DE CORREO 13
4 ¿QUÉ SIGUE? **16**
5 CONCLUSIONES **18**
6 REFERENCES **20**
APÉNDICE A - CONFORMACIÓN DEL GRUPO DE SEGURIDAD **22**
APÉNDICE B – TABLA DE IDENTIFICACIÓN DE RECURSOS **26**
APÉNDICE C – MATRIZ DE VALORACIÓN DE ACTIVOS **28**

© SANS Institute 2004, Author retains full rights.

1 ABSTRACT

Cada día dependemos más de Internet tanto a nivel personal como empresarial; en el hogar para realizar labores tan sencillas como enviar un correo electrónico a un familiar, consultar las noticias del día, reservar unas entradas para el cine o pagar los servicios públicos; en la oficina, para poder ofrecer y vender los servicios que se prestan, para poder tener contacto rápido y confiable con los proveedores y clientes, y en general para tener una comunicación ágil que le permita obtener unos grandes beneficios y utilidades. Es aquí donde vemos que la seguridad juega cada vez un papel más importante, intentando garantizar la confidencialidad e integridad de la información que se maneja, y la disponibilidad de los servicios que se prestan, siendo más importante aún sobre los ISP's (Internet Service Providers), los cuales se encargan de prestar los servicios de conexión a Internet, correo electrónico, publicación de páginas Web, entre otros, sirviendo de herramienta de comunicación tanto a hogares como a empresas.

Cada vez son más compañías las que toman conciencia del papel crítico que juega la seguridad informática, pero en ocasiones la falta de recursos económicos o humanos llevan a designar estas labores a personas sin conocimiento o experiencia en el tema, haciendo que los tiempos de establecimiento de los procesos y procedimientos de seguridad necesarios para mantener el funcionamiento normal de los servicios no sea el adecuado. Uno de los grandes dilemas que enfrenté cuando me asignaron como Oficial de Seguridad para un ISP, fue el de determinar por donde comenzar a establecer la seguridad de la empresa. Es una pregunta difícil de contestar, y más cuando los servicios típicos como son acceso remoto, correo, páginas Web, entre otros, ya se están prestando y los conocimientos en seguridad informática son mínimos. Si está pensando en establecer un grupo de seguridad para un ISP, o si usted ha sido designado para establecer la seguridad y no tiene el conocimiento o la experiencia necesarios, espero que este documento le sea de gran utilidad como guía práctica en la búsqueda de su objetivo. A lo largo del paper se verán algunos de los errores y aciertos que se tuvieron en el establecimiento de la seguridad del ISP, cómo iniciar el proceso de seguridad si ya se tienen en funcionamiento los servicios, cuales son algunos de los pasos a seguir para mantener una seguridad mínima y cómo generar un plan de seguridad. Aunque el documento está orientado a un ISP, se pueden tomar algunas de estas ideas para aplicarse sobre un ambiente corporativo.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2 ¿CÓMO COMENZÓ LA SEGURIDAD EN EL ISP?

A lo largo del proceso de implementación del ISP se enfocaron la mayor cantidad de esfuerzos a establecer los servicios que se iban a prestar a los clientes: conexión a Internet, correo electrónico, páginas Web personales y el portal del ISP.

En ese momento, la seguridad informática no jugaba un papel crítico dentro de la organización y se tuvieron en cuenta algunos parámetros básicos: un firewall para separar los equipos de Internet, y una arquitectura de frontend - backend, la cual permitía proteger los servidores que prestan servicios hacia Internet, ubicados en una VLAN de front-end y aquellos en los que se tenía la información crítica de los usuarios ubicados en una VLAN de back-end. Adicionalmente, los servicios de correo, DNS y WEB, se configuraron basados en las mejores prácticas. Algo bueno para comenzar, sin tenerlo claro se trabajaron conceptos importantes de Defensa en profundidad, centrando esfuerzos en algunos niveles como: 1) información: generando una arquitectura que separó y protegió la información más crítica de un contacto directo con Internet, 2) aplicación: configurando de manera adecuada y no con los valores por defecto cada uno de los servicios que se prestarían hacia Internet (DNS, WEB, SMTP, POP, IMAP), 3) red, generando redes privadas para los servidores y separándolas de las redes públicas, mediante un firewall que permitía controlar el tráfico dirigido hacia ellos y encargado de hacer la traducción de la IP pública a la IP privada correspondiente (NAT - Network Address Traslation[1]) para que los paquetes llegaran finalmente a la red privada.

En ningún momento se establecieron roles y responsabilidades claras, ni tampoco una persona o grupo encargado de la seguridad. Las únicas responsabilidades que se dejaron establecidas fueron las de creación y modificación de reglas del firewall, las cuales quedaron a cargo del administrador de servidores y servicios.

Seis meses después del inicio del ISP, se vio la necesidad urgente de separar roles y responsabilidades y de crear un grupo de seguridad aparte de los grupos de soporte, proyectos, redes y servicios. Yo trabajaba en el grupo de servidores y servicios, contaba con conocimientos de redes y desarrollo de software, pero no en seguridad; no había candidatos para este grupo y la contratación de una persona externa en la empresa podría llegar a tardar más de seis meses, razón por la cual me fue asignada esta responsabilidad. Fue un gran reto para mí, pero un gran riesgo para la empresa debido a que el conocimiento y la experiencia son factores fundamentales para la implementación de un plan de seguridad, características con las cuales no contaba. Es un grave error asignar estas responsabilidades a una persona que no tiene el conocimiento, esto conlleva a que el tiempo de establecimiento de la seguridad sobre la compañía tome más tiempo (mientras la persona o grupo asignado adquiere el conocimiento y lo implementa), y que durante este tiempo se corra el riesgo de perder información vital para la empresa o para los clientes o de afectar el servicio sin contar con una forma rápida de recuperarse.

Comencé a investigar y me encontré con un gran mar de información sobre el cual casi naufrago: el papel del oficial de seguridad, herramientas de seguridad para todo tipo de cosas, auditoria, planes de continuidad del negocio, planes de recuperación, manejo de incidentes, aseguramiento de servidores, instalación de parches, seguridad en redes, firewall,

[1] http://www.faqs.org/rfcs/rfc1631.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

análisis de riesgos, BCP, DRP, RFC's, COBIT, ISO 17799, NIST, CERT y un sin fin de temas y sitios que no permitían conocer la respuesta al dilema que tenía cuando me asignaron este rol: "¿Por dónde empezar?"

En muchos de los sitios de información aparece como factor común que la base de la seguridad informática son las políticas y procedimientos. El perfil técnico en el que me venía desenvolviendo, no me permitió entender su utilidad, ni importancia, razón por la cual decidí comenzar por aprender qué tipos de ataques existen y qué herramientas se utilizan para estos, para así conocer al enemigo y saber de qué nos debíamos proteger. Desde aquí inició un gran camino, en el cual no contaba con una visión global de la seguridad y cuyo foco principal siempre fue la parte técnica.

Los primeros esfuerzos para mejorar la seguridad del ISP se centraron en el aseguramiento de los servidores, basado en la información de CERT Security Practices[2] y los cinco pasos recomendados: Hardening/securing, prepare, detect, response, improve. Este aseguramiento hizo que la avalancha de gusanos como Nimda y CodeRed no causaran ningún tipo de afectación.

Posteriormente, dentro de la selva de información apareció el RFC 3013[3] "Recommended Internet Service Provider Security Services and Procedures", el cual fue de gran utilidad para identificar algunas grandes falencias como la información de contacto que se debía tener, filtros de entrada y de salida, manejo de incidentes, Appropriate Use Policy (AUP). Este RFC sirvió como un gran paso para comenzar a mejorar la seguridad del ISP.

Después de esto, se trabajó en la implementación del sistema de respaldo y recuperación con el fin de disminuir el riesgo de perder la información que se tenía en los servidores, y adicionalmente contar con la posibilidad de recuperar un servidor en caso de desastre en el menor tiempo posible. De manera simultánea, se trabajó en la integración del sistema de antivirus a la plataforma de correo.

La cantidad de temas sobre los que estaba trabajando y todos los que quedaban pendientes por mejorar hicieron necesario pensar en crear un grupo de seguridad que soportara las necesidades del ISP. La creación de la estructura de seguridad, la definición de los roles y responsabilidades, y la justificación de cada uno de los integrantes del grupo de seguridad fue basada en la sección "Establishment of a suitable organisational structure for IT security"[4] del "IT Baseline Protection Manual". El detalle completo del grupo de seguridad se puede encontrar en el APÉNDICE A - CONFORMACIÓN DEL GRUPO DE SEGURIDAD.

El número de reclamos que llegaban de Internet por el comportamiento inadecuado de algunos de nuestros clientes (spam, gusanos, etc.), hizo evidenciar la gran falla por no contar con unas políticas de uso aceptable. No podíamos tomar ninguna acción, ni exigir la corrección a estos inconvenientes al cliente, por no tener definido que tipo de comportamiento estaba permitido o prohibido, resultaba legalmente imposible tomar las medidas correctivas del caso. Al volverse un punto crítico fue necesario definir, establecer y publicar una política de uso aceptable, tomando como fuente los ejemplos de SANS[5] y de ISP's reconocidos a nivel mundial, que sirviera como base para que los clientes prestaran la atención necesaria para mejorar la seguridad de sus redes; cabe aclarar que fue necesario

---

[2] http://www.cert.org/security-improvement/index.html
[3] http://www.faqs.org/rfcs/rfc3013.html
[4] http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/s/s2193.htm
[5] http://www.sans.org/resources/policies

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

realizar un trabajo conjunto con el área comercial y jurídica, quienes dieron su aprobación para que se adicionara como parte del contrato que se establece con los clientes.

Finalmente, se implementaron los proyectos de aseguramiento de servidores y el de detección de intrusos (IDS). El primero con el fin de realizar un endurecimiento a cada uno de los servidores con los que cuenta el ISP, y el segundo con el fin de contar con una herramienta que apoye la detección de ataques hacia los equipos del ISP, los ataques de los clientes hacia Internet y de Internet hacia nuestros clientes.

Aunque se contaba con herramientas para mejorar la seguridad, algunas de ellas no funcionaban de la forma en que se esperaba. En ocasiones se requería recuperar la información de un servidor y no era posible debido a que la cinta en la que se había guardado presentaba problemas, o por que el backup realizado había fallado por alguna razón. En el caso de la herramienta antivirus, eran tantos los correos generados por los nuevos tipos de gusanos y las nuevas técnicas de spam que sobrecargaban los servidores haciendo que las colas de correo crecieran hasta el punto de causar la caída del servicio y por ende generando afectaciones a los clientes. Adicionalmente, se tiene configurado el servicio de DNS sobre algunos de los servidores de correo, causando que se degradara el servicio de navegación debido a la respuesta lenta de los servidores.

El trabajo realizado a lo largo de dos años con el fin de mejorar la seguridad del ISP no tenía un resultado tangible, se adquirieron herramientas sin tener una claridad de cuanto realmente sería el beneficio, se llevaron a cabo una serie de actividades sin un criterio que permitiera identificar en qué paso estábamos y cuál sería el próximo paso a seguir, no existía un plan de seguridad. El único criterio que en algunas ocasiones se tenía era el de solucionar los problemas urgentes que se estaban presentando.

Todo esto hizo que aunque se contara con una inversión importante en seguridad, no se tuviera un resultado visible, que permitiera conocer la ganancia obtenida en la búsqueda de generar una continuidad del negocio, confirmando así una de las grandes frases que a diario se repiten en esta área: “La seguridad no es una herramienta, es un proceso”

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3 MEJORANDO LA SEGURIDAD DEL ISP

La cantidad de temas cubiertos durante el curso, tocando desde los aspectos técnicos, hasta aspectos legales, permitieron ver la seguridad de una forma más amplia y entender cómo entran a jugar un papel importante aspectos que parecen fuera de este contexto (rutas de evacuación, documentos de procedimientos, auditoria) y que desde el punto de vista netamente técnico parecen no tener relevancia en el establecimiento de la seguridad. Entender el funcionamiento de todas estas piezas permitió organizar, planear y generar un plan de seguridad acorde con las metas del negocio, dándole una mayor prioridad a las actividades que realmente generan un mayor impacto dentro de la empresa.

Para generar un plan de seguridad que permitiera rápidamente mejorar la seguridad del ISP se realizó un análisis de riesgos básico en conjunto con la Gerencia de Datos, la cual está encargada de los servicios de datos y de Internet. ¿Por qué con la Gerencia? Por que son ellos los que conocen el negocio y los que definen los parámetros de mayor relevancia, los cuales muy probablemente van a ser diferentes a los que se tienen desde el punto de vista técnico. Esta es una de las razones importante de tener un contacto directo con la gerencia en el desarrollo e implementación del plan de seguridad de la empresa.

La meta principal de la Gerencia es la prestación adecuada de los servicios a los clientes, cumpliendo con los acuerdos de niveles de servicio ofrecidos. En el APÉNDICE B – TABLA DE IDENTIFICACIÓN DE RECURSOS se resumen algunos de los principales servicios que se prestan y los recursos en los que se apoyan estos servicios para funcionar, los cuales sirvieron de primer acercamiento para el desarrollo del análisis.

Aunque la facturación juega un papel importante dentro de la empresa, es un tema que lo ha venido trabajando otra gerencia y que se lo ha manejado desde hace mucho tiempo para la parte de servicios de telefonía local, razón por la cual no se tuvo en cuenta dentro de este estudio.

Después de identificar los activos importantes de la empresa, se generó una matriz de valoración de los activos (ver APÉNDICE C – MATRIZ DE VALORACIÓN DE ACTIVOS), con el fin de determinar los aspectos críticos del negocio. Una vez identificados estos recursos, se centraron los esfuerzos en analizar y mejorar la seguridad de los puntos más críticos, como alcance inmediato y posteriormente programar la realización de un análisis de riesgos detallado de forma periódica para mantener un mejoramiento continuo.

El análisis se realizó tomando como base los principios básicos de la seguridad: Confidencialidad, Integridad y Disponibilidad.

3.1 Recurso Humano

En la matriz se puede observar que el recurso humano es el factor más importante dentro de la Gerencia, razón por la cual es necesario trabajar en su protección.

Confidencialidad:

El conocimiento del negocio y el acceso a información privilegiada son los principales aspectos. En el contrato que firma cada empleado existe una cláusula de confidencialidad como base para evitar fugas de información. En cuanto a la información que se maneja, es necesario trabajar en su identificación y clasificación.

Integridad:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

La seguridad de las personas y de su integridad es el factor más crítico dentro de la empresa, ya que es en ellas donde reside el conocimiento del negocio y permiten su funcionamiento. El conocimiento y experiencia que se tiene en este aspecto por parte del grupo de seguridad es mínimo, razón por la cual se delegó esta labor al área de planta física de la empresa. Esta área ya había desarrollado un plan sobre la Gerencia, pero el crecimiento de personal y de instalaciones en los últimos dos años lo volvieron obsoleto, siendo necesario y urgente su replanteamiento. Durante el seguimiento que se ha venido realizando, se ha visto que los elementos de detección (detectores de humo) y de supresión (extinguidotes) existen y se les realiza un control periódico. La parte que se encuentra débil actualmente es el plan de evacuación, ya que no existen rutas de evacuación, definición de roles durante la emergencia, señalización que permita una rápida evacuación, puntos de encuentro, realización de simulacros y demás aspectos vitales en caso de una emergencia, tareas en las que se encuentra trabajando planta física.

Disponibilidad:

La continuidad del negocio depende totalmente de sus empleados y es normal que ocurran eventos que puedan llegar a causar su ausencia. Actualmente la gerencia y los mismos empleados generamos backup en los roles y responsabilidades, con el fin de evitar que el conocimiento este en cabeza de pocos y permitiendo que las personas puedan tomar sus periodos de descanso sin problema.

3.2 DNS

Sobre este servicio realicé una revisión detallada de los puntos de falla y debilidades existentes, teniendo en cuenta la importancia de este servicio para el ISP ya que es la principal actividad que se presta a los clientes. Este análisis fue basado en el documento del NIST "Domain Name System Security Technical Implementation Guide"[6].

Antes de entrar en detalle dentro del análisis, vale la pena indicar los tipos de servidores de nombre que se tienen:

- Autoritativos: guardan los registros de las zonas para uno o más dominios y se encargan de dar respuesta a otros servidores sobre los dominios que tiene configurado. Existen dos clases: primario maestro y esclavos. Puede existir uno o más esclavos y estos se actualizan con el primario mediante una transferencia de zonas.
- Servidores de resolución: se encargan de resolver peticiones realizadas por clientes. Pueden hacer resolución de nombres por dos métodos: recursión o forwarding. En el primer método busca primero en su cache a ver si tiene el registro solicitado por el cliente y si no lo tiene consulta con los servidores autoritativos para ese dominio, una vez obtiene la respuesta se la entrega al cliente. Los de forwarding, se encargan de reenviar el requerimiento a otro servidor para que este haga la consulta.

Actualmente se tienen dos servidores de DNS. Uno está como autoritativo maestro y el otro como autoritativo esclavo, y los dos están como servidores de resolución de tipo recursión, atendiendo los requerimientos de los clientes. Allí se mantiene la información de las zonas pertenecientes al ISP y a los clientes que han solicitado este servicio. En estos servidores también se presta el servicio de smtp, para recibir correos de Internet en el primero y para que los clientes envíen sus correos en el segundo. Estos servidores se encuentran protegidos por el sistema de firewall.

[6] http://csrc.nist.gov/pcig/STIGs/DNS-STIG-V2R1A.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Existen también otros dos servidores de DNS internos, que se encargan de manejar y resolver los nombres de equipos que se encuentran en el dominio interno. Estos servidores se encuentran en una red privada interna (back-end), aislados totalmente del mundo exterior.

Confidencialidad:

Es importante que la información de las zonas no sea robada, ni que personas externas tengan acceso a la información de las redes internas. Como aspectos positivos se tiene que los servidores tienen configurado únicamente la transferencia de zonas entre ellos, restricciones en el firewall para esto, el DNS se ha configurado con las recomendaciones del fabricante, a los servidores se les ha realizado un aseguramiento (instalación de parches y endurecimiento) y se cuenta con una separación del DNS interno y externo (SPLIT DNS).

Se detectó una gran debilidad al tener sobre los mismos servidores de DNS el servicio de SMTP. Al estar compartiendo los recursos se corre un gran riesgo si alguno de los dos servicios es vulnerado, exponiendo la información que se tiene del DNS.

Integridad:

En el DNS es crucial garantizar la integridad de la información, ya que si un intruso puede modificar la información, podría redirigir a los clientes a un sitio controlado por este y robar información. Al igual que en el caso anterior, al tener el servicio de SMTP se estaría exponiendo a que si este servicio es vulnerado y se tiene acceso a la máquina se podría atentar contra la integridad del DNS, modificando algunos registros. Adicionalmente, se deben evitar ataques de envenenamiento de cache que permitan alterar la información que se tiene, para lo cual se tuvieron en cuenta algunas recomendaciones de Microsoft[7].

Disponibilidad:

En este punto es donde más impacto se tiene con el cliente, ya que su principal actividad es la navegación. Si se llegaran a tener problemas con este servicio, de inmediato se generaría una avalancha de llamadas y reclamos.

Aunque se cuenta con una redundancia al tener dos servidores, no cumple con las necesidades y niveles de disponibilidad que se le deben garantizar al cliente. En varias ocasiones se ha presentado degradación en el servicio de navegación, causado por la lentitud en el tiempo de respuesta a los requerimientos de DNS debido a que los servidores se encuentran sobrecargados por la cantidad de correo SPAM o gusanos, y que en ocasiones llegan incluso a causar su caída. Adicionalmente, al estar los servidores ubicados física y lógicamente en el mismo segmento lo hacen un punto bastante vulnerable, en algunas oportunidades se han tenido problemas con el sistema de firewall que causan de inmediato una afectación del servicio a los clientes. También existe una debilidad al tener sobre cada equipo de DNS los servicios autoritativos y de resolución, ya que al no diferenciar y monitorear el tipo de tráfico, se pueden recibir diversos ataques sin poderlos detectar ni prevenir.

Teniendo en cuenta lo anterior y basado en la guía del NIST, diseñé una arquitectura que permitiera mejorar las debilidades expuestas y que aumentara el nivel de disponibilidad del servicio. En la Gráfica 1 Arquitectura DNS se encuentra la propuesta realizada, la cual cuenta con las siguientes características:

- Se tienen servidores dedicados a DNS

[7] http://support.microsoft.com/default.aspx?scid=kb;EN-US;241352

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Se separan los servidores por funciones que permitan diferenciar el tipo de solicitudes que va a atender:
    - Un servidor como autoritativo primario (Autoritativo 1) y otro como autoritativo esclavo como contingencia, los cuales se encargan de dar respuesta a otros servidores (Flechas rojas D1) y en los cuales la cantidad de requerimientos debe ser pequeña, siendo fácil detectar ataques de tipo de negación de servicio mediante la revisión del tamaño del log. (Ver flechas rojas D1)
    - Dos servidores de resolución de tipo forwarding (Forward 1 y Forward 2), recibiendo las peticiones de los clientes (flecha 1), y reenviando las solicitudes a los servidores de recursión (flecha 2) y una vez obtienen la respuesta (flecha 5) se la entregan a los clientes (flecha 6). El acceso a estos servidores está permitido únicamente a los clientes, disminuyendo notablemente la cantidad de posibles atacantes.
    - Dos servidores de resolución de tipo recursión (Cache 1 y Cache 2), los cuales se encargan de realizar peticiones a otros servidores en Internet (flecha 4) cuando no encuentran la respuesta a la consulta de DNS en su cache; una vez obtienen la respuesta se la entregan a los servidores de forwarding (flecha 5), quienes finalmente se la envían al cliente. El acceso a estos servidores no está permitido desde Internet, son ellos los únicos que pueden generar requerimientos, minimizando la posibilidad de exposición de estos equipos a ataques que permitan a un intruso modificar algún registro.

      Las flechas azules de la gráfica muestran el requerimiento desde que sale del cliente y llega hasta el servidor que genera la respuesta final. Las flechas negras muestran el camino de regreso con la respuesta, hasta su llegada al cliente.

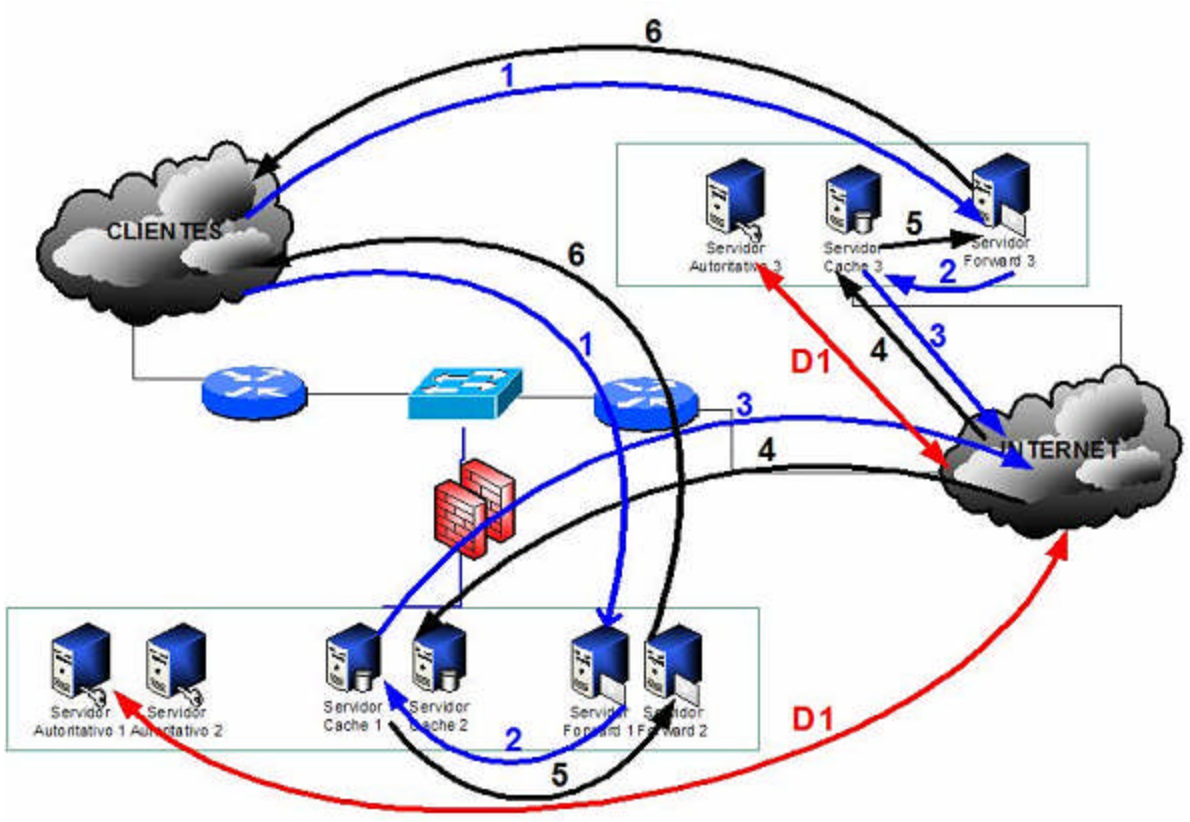
      En el switch se puede configurar para que balancee la carga de cada pareja de servidores, permitiendo que si se cae alguno el otro continúe respondiendo los requerimientos de los clientes de forma transparente.
    - Se tienen tres servidores más de DNS (Autoritativo 3, Cache 3 y Forward 3) en un sitio alterno separado física y lógicamente del principal, atendiendo requerimientos de la misma forma que los descritos anteriormente, generando una redundancia adicional en el servicio.
- Se mantiene el esquema de DNS split, dejando servidores separados de Internet para los servicios de DNS interno.

Adicionalmente, se recomendó a los administradores del DNS tener en cuenta el RFC 1912 "Common DNS Operational and Configuration Errors"[8], el uso de algunas herramientas descritas en el RFC 1713 "Tools for DNS Debugging"[9], con el fin de automatizar el proceso de cambios en el DNS y realizar un monitoreo del comportamiento de los servidores, estableciendo mecanismos no solo de prevención, sino también de detección.

[8] http://www.faqs.org/rfcs/rfc1912.html
[9] http://www.faqs.org/rfcs/rfc1713.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Para los servidores de DNS se recomendó utilizar el servicio de BIND 9, el cual se puede obtener gratis en http://www.isc.org, ya que ha sido ampliamente probado por DISA (Defense Information System Agent) y ha sido re-escrito totalmente pensando en seguridad.



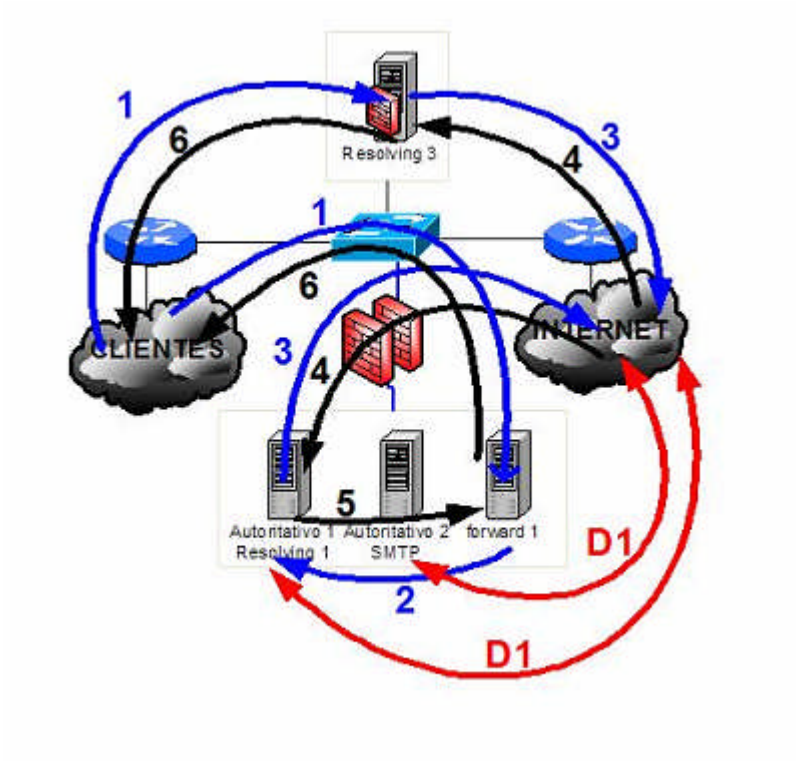
Gráfica 1 Arquitectura DNS

En la gráfica no se representa la redundancia de enrutadores y switches por practicidad.

Un documento completo del DNS y la arquitectura propuesta fue presentado a la Gerencia para su aprobación, pero debido a la cantidad de máquinas requeridas y al presupuesto con el que se contaba fue necesario generar un nuevo diseño que se acogiera a los recursos que se tenían. El diseño finalmente aprobado se encuentra en la Gráfica 2 Diseño aprobado. Actualmente el área de servicios se encuentra trabajando en la implementación del diseño aprobado, en conjunto con el grupo de analistas de seguridad. A un mediano plazo, se piensa implementar una redundancia total de los servicios principales en un centro de computo alterno, sobre el cual se terminaría de implementar el diseño planteado originalmente.

Dentro de la arquitectura aprobada se mantuvieron algunas debilidades como la de tener el servicio de SMTP y DNS sobre uno de los servidores. En este caso quedaron uno externo (resolving 3) y dos internos (forwarding1 y resolving 1). Para controlar el acceso al DNS externo se va a configurar un firewall en la máquina y adicionalmente se van a crear listas de acceso en los enrutadores de frontera para permitir únicamente llegada de requerimientos al puerto 53.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Gráfica 2 Diseño aprobado

3.3 Acceso Físico

EL control de acceso físico es uno de los que más fácil se pueden llegar a olvidar si el análisis se limita a la parte técnica. Es la base para que los demás controles que se tengan no sean vulnerados, se encuentra en el nivel 1 de la capa OSI y se le debe prestar la atención adecuada.

Confidencialidad:

Como primera medida de control se tiene la portería, en la cual solo el personal autorizado puede ingresar al edificio, infortunadamente la cantidad de personas que deben ingresar es bastante grande, pudiendo fácilmente tener acceso a las tres áreas principales: una con los servidores, enrutadores y otros equipos de conmutación y transmisión, otra de centro de gestión, en la que se encuentran los operadores y en donde se realiza el monitoreo y gestión de los servicios y equipos, y una última en donde se encuentran las oficinas. Estas áreas no tenían ningún tipo de señalización que permitiera claramente identificar las zonas en las que el acceso es restringido. Existen puertas separando las tres áreas y un sistema de tarjetas con control de acceso, pero mantienen abiertas o las tarjetas son prestadas o para permitir el acceso a terceros se les deja abierto y no se realiza un acompañamiento durante el desarrollo de esta actividad.

Integridad:

Durante el año se presentaron desconexiones en algunos equipos y se perdió un disco duro de un servidor de pruebas, evidenciando las grandes falencias de políticas de seguridad física, de control y monitoreo. Se había solicitado presupuesto para implementar sistemas de monitoreo y protección para los equipos, pero no fue aprobado y no se pudieron tomar medidas.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Adicionalmente, se empezaron a presentar problemas debido a que no se tenía un procedimiento establecido para el ingreso de nuevos equipos a la red, razón por la cual en algunas ocasiones las personas que estaban implementación un nuevo proyecto o necesitaban realizar una prueba conectaban sus equipos a los switches, pudiendo llegar a ocasionar problemas en la red.

Disponibilidad:

Cuando el sistema de tarjetas presenta problemas se tiene la posibilidad de ingresar con un sistema de llaves, las cuales son administradas por el coordinador del centro de gestión. También se cuenta con puertas de emergencia que permiten tener un punto de acceso y salida en caso de problemas.

Para el presupuesto solicitado para el próximo año se va a incluir nuevamente el proyecto de seguridad física, pero esta vez con una base más fuerte y apoyados sobre el estudio realizado. Como medida inmediata, se generó la política de seguridad física, en las que se establecen los niveles de acceso, el acompañamiento que se debe realizar a terceros y se estableció que las puertas deben mantener cerradas. Adicionalmente se generó una señalización que permitió identificar las zonas a las que se puede tener acceso libremente y a las que no.

Para evitar la conexión indiscriminada de equipos en los switches y en general en la red del ISP, fue necesario establecer una política de ingreso de nuevos equipos, en los que se establecía como parte principal la revisión y aseguramiento por parte del área de seguridad y se generaron controles de validación por dirección MAC a nivel de puertos en los switches[10].

3.4 SERVIDORES DE CORREO

En el cuarto lugar aparecen los servidores de correo, punto que cada día se vuelve más crítico debido a la cantidad de reclamos que se reciben de los clientes que se quejan por la cantidad de correos diarios de spam y de virus que aparecen en sus casillas.

Confidencialidad:

El manejo de contraseñas que tienen algunos clientes del ISP permite que sean fácilmente determinados y que por tanto puedan llegar a acceder a sus buzones de correo. Esto también genera un gran problema sobre los servidores, debido a que el mecanismo de envío de correos para los clientes se realiza por medio de autenticación, dejándole abierta la posibilidad para que una vez autentique pueda enviar cualquier tipo de correo.

En cuanto al acceso a los correos de los usuarios, únicamente lo pueden hacer el administrador del sistema, para realizar labores de mantenimiento y seguimiento a problemas y el responsable de manejo de incidentes, para sacar información solicitada por entidades judiciales.

---

10 http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800da706.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A nivel de protocolos de comunicación, no se han implementado SMTP, ni POP seguros con el fin de garantizarle al cliente que nadie más pueda ver su información mientras cruza la red.

Integridad:

No se tiene implementado ningún mecanismo de firmas digitales que permita a los usuarios garantizar la no alteración de sus mensajes.

Disponibilidad

En varias ocasiones se presentaron problemas de SPAM generado desde nuestros servidores, debido a que algunos atacantes, mediante técnicas de diccionario lograban obtener usuarios y contraseñas fáciles de identificar. Una vez obtenían la clave, se autenticaban con ese usuario y generaban la mayor cantidad de correos que podía, desde diferentes sitios. Esto hizo que nos reportaran en listas negras durante una semana, lo cual causó una gran afectación en el servicio.

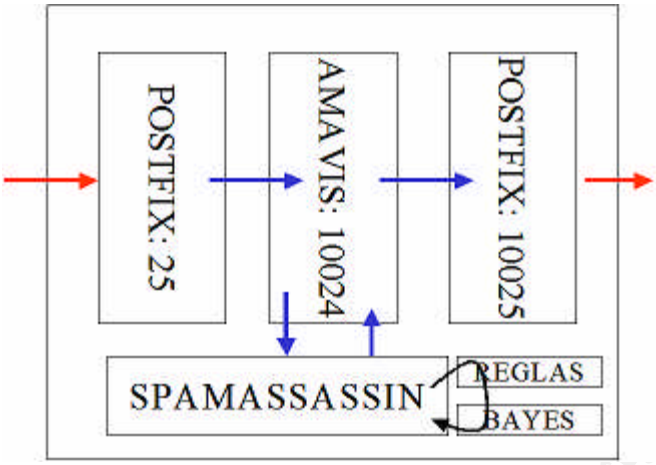
La cantidad de correos SPAM y correos con virus han causado que en ocasiones las colas de correo crezcan hasta el punto de no soportar la carga y que se caigan los servidores.

Para mejorar estos aspectos, se trabajó inicialmente en una campaña de educación a los clientes, en las que se les envió un correo indicando las ventajas de tener una contraseña fuerte y algunas técnicas para fácil recordación. También se realizaron cambios en las páginas en donde se establecen las contraseñas, con el fin de realizar un primer filtro en el que se compara contra unas reglas básicas y se le avisa al usuario en caso de ser una clave débil.

Se venía adelantando un proceso de contratación de una solución de antivirus y antispam, pero el tiempo estimado para su implementación excedía los seis meses, razón por la cual se decidió implementar rápidamente un sistema antispam basado en software libre. En conjunto con un analista de seguridad investigamos diferentes opciones y finalmente encontramos una página publicada por Scott L. Henderson[11], en la que explicaba paso a paso cómo realizar la implementación de un sistema de correo sobre linux, con postfix como manejador de las colas de correo, amavis como administrador de contenido y spamassassin encargado de generar un peso a los correos para determinar si era posible correo basura o no. En la Gráfica 3 se ilustra el camino que sigue el correo electrónico una vez llega al servidor, quién finalmente lo entrega a los servidores de correo de Microsoft Exchange.

[11] http://www.geocities.com/scottlhenderson/spamfilter.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Gráfica 3

La implementación de este sistema duró tres semanas y se realizó sobre un solo servidor, el cual fue configurado como MX, para controlar los correos que estaban llegando desde Internet hacia los usuarios. Se crearon filtros básicos para evitar algunos gusanos, revisando por archivos con doble extensión, con extensión peligrosa (.pif, .com, .scr, .vbs), se activaron verificaciones del protocolo, aprendizaje bayesiano, uso de listas negras, entre otros.

No se contaba con más máquinas para generar redundancia, permitiendo así que actuaran como gateway de correo y realizaran la revisión total, así que quedaron configurados dos servidores como MX: el que instalé y uno que venía trabajando antes como MX normal. Las estadísticas empezaron mostraban un nivel de detección inicial del 4% diario (2.000 – 4.000) y dos meses después subieron a un 15% (15.000 – 18.000), notándose un incremento sustancial en el número de correos recibidos por día.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4 ¿QUÉ SIGUE?

Como medida final, teniendo en cuenta algunos aspectos de defensa en profundidad y buscando generar seguridad por capas, se revisaron algunos niveles del modelo OSI, listando las medidas tomadas hasta el momento e intentando detectar otras más que quedarían pendientes por realizar para minimizar las vulnerabilidades existentes.

Nivel Físico

Hasta el momento se han implementado las siguientes medidas:

- Creación de avisos que permitan diferenciar claramente las zonas restringidas.
- Revisión del plan de seguridad orientado al personal (safety)
- Generación de las políticas generales de seguridad, de las cuales se desprenden las siguientes políticas:
  - Política de acceso a la información
  - Política de seguridad físico
  - Política de seguridad de Red
  - Política de seguridad de los sistemas, la cual incluye acceso remoto, instalación de nuevos equipos y aseguramiento de sistema operativo.
  - Política de uso aceptable

Quedan pendientes por realizar:

- Rediseño del plan de seguridad orientado al personal (safety)
- Aprobación y divulgación del documento de Administración de Cambios, en el cual se incluyeron las políticas de seguridad
- Entrenamiento a los funcionarios en Seguridad
- Generación y divulgación del portal de seguridad del ISP para apoyar a los clientes
- Solicitud de presupuesto para realizar el proyecto de seguridad física que busca generar prevención mediante mecanismos de control de acceso sobre los servidores y equipos de red, y mecanismos de detección para monitorear la entrada y salida de las diferentes áreas.
- Identificación y clasificación de la información
- Generación de las demás políticas y procedimientos.
- Actualización del inventario de equipos y sistemas

Nivel de Enlace

Hasta el momento se han implementado las siguientes medidas:

- Seguridad por dirección MAC en los puertos de los enrutadores
- Redundancia de switches, minimizando el impacto en caso de falla de uno de ellos. La mayoría de servicios y equipos se tienen redundantes, de tal forma que cada uno se conecta a un switch diferente.
- Pruebas de vulnerabilidades a los switches y generación de la guía de aseguramiento.

Quedan pendientes por realizar:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Separación física de las VLANS, ya que tanto las VLANS privadas como la de Internet se encuentran sobre los mismos equipos, exponiendo toda la información privada.
- Identificación y generación de políticas para los equipos de transmisión
- Generación de los procedimientos de auditoria a estos equipos

Nivel de Red

Hasta el momento se han implementado las siguientes medidas:

- Firewall de frontera
- Direccionamiento privado para los servidores.
- Creación de filtros en los enrutadores de frontera, para evitar la propagación de virus
- Creación de filtros en los enrutadores de los clientes y equipos concentradores de acceso como TNT, para evitar propagación de virus entre clientes.
- Realización de pruebas de vulnerabilidades y generación de la guía de aseguramiento
- Detectores de Intrusos a nivel de Red
- Gestión y monitoreo de los elementos de Red.
- Redundancia de los equipos críticos

Quedan pendientes por realizar:

- Generación de los procedimientos de auditoria a los enrutadores de borde y de los clientes
- Definición e implementación de los procedimientos de monitoreo y reacción de los ataques detectados por el IDS de red

Nivel de Aplicación

Hasta el momento se han implementado las siguientes medidas:

- Realización de pruebas de vulnerabilidades y generación de la guía de aseguramiento
- Aseguramiento de los servidores que prestan servicios a Internet, tanto a nivel de sistema operacional como de aplicación
- Detectores de Intrusos a nivel de host
- Gestión y monitoreo de los servicios que se prestan a clientes
- Generación de backup de los servidores

Quedan pendientes por realizar:

- Aseguramiento de la totalidad de servidores
- Aseguramiento equipos del personal de la Gerencia
- Implementación del sistema de antivirus y antispam contratado
- Implementación de la arquitectura para el servicio de DNS aprobada
- Generación de los procedimientos de auditoria a los servidores y servicios
- Implementación de los procedimientos de monitoreo y reacción de los ataques detectados por el IDS de host
- Definir una guía de desarrollo de software seguro

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Definir la lista de chequeo para los servidores, equipo de red y aplicaciones que van a ingresar a la red.

Aquí se pueden ver algunas de las muchas actividades que están pendientes por realizar, siendo necesario darles una prioridad con el objetivo de implementarlas de tal forma que mejoren la seguridad alineados con las metas de la empresa.

En este momento inicia el ciclo de seguridad en el que continuamente vamos a estar analizando el estado actual, planeando la forma de mejorar, implementando estas mejoras, auditando el cumplimiento de los procesos y procedimientos definidos, entrenando a las personas involucradas y volviendo a iniciar el ciclo, todo unido en el plan de seguridad.

5 CONCLUSIONES

Cuando se quiere iniciar el proceso de seguridad de la compañía en la cual ya se tienen unos servicios montados y no se ha tenido en cuenta la seguridad dentro de su implementación, es necesario realizar un plan inmediato que permita mejorar lo más crítico en el menor tiempo.

El procedimiento que se siguió para realizar esto se resume así:

1. Identificación de las metas del negocio.
2. Identificación de los servicios críticos y los activos en los que se soportan.
3. Evaluación del impacto de los activos identificados sobre las metas del negocio, en este caso sobre los servicios ofrecidos a los clientes.
4. Análisis del estado de la seguridad de los activos identificados como de mayor criticidad.
5. Realizar las mejoras identificadas en el análisis anterior
6. Definir políticas iniciales

Es importante anotar que independientemente de este estudio, es de vital importancia que todos los servidores que están expuestos a Internet, tengan al menos un firewall que los proteja y estén asegurados (con los últimos parches, configurados de forma correcta, con la menor cantidad de permisos, ...). En este caso se contaba con el firewall y ya se venía adelantando un proceso de aseguramiento de servidores, razón por la cual no se entró en detalle de estas actividades.

Una vez se tiene identificado y controlado lo urgente es necesario pasar a lo importante, generando un plan de seguridad que permita administrar, manejar y controlar los riesgos que se tienen.

No existe una regla general que permita determinar el plan de seguridad de una empresa, ya que depende del foco del negocio, el nivel de madurez y los procesos y procedimientos que se tengan al interior. Existen varias metodologías alrededor del tema, pero la gran mayoría se basan en la evaluación del riesgo.

ISO 17799 es un estándar que define los 10 dominios a trabajar para mejorar la seguridad de la empresa y el BS7799-2 especifica una metodología para su implementación.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Adicionalmente, existen herramientas como COBRA[12] que apoyan la evaluación de la implementación de este sistema.

El CERT cuenta con una metodología flexible llamada OCTAVE[13] (Operationally Critical Threat, Asset, and Vulnerability Evaluation), orientada a grandes empresas y está en desarrollo de otra orientada a pequeñas empresas.

El NIST (The National Institute of Standards and Technology), a través de su CSRC (Computer Security Resource Center)[14] se encuentra en continua investigación y desarrollo de nuevos estándares y guías que permitan apoyar a las empresas en la planeación, implementación, administración y operación de las tecnologías de información de una forma segura, es así como en 1998 desarrolló una guía orientada a la creación de un plan de seguridad: "Guide for Developing Security Plans for Information Technology Systems"[15], y posteriormente desarrolló una guía basada en controles: "Recommended Security Controls for Federal Information Systems"[16]

Es necesario apoyarse en alguna de las metodologías existentes con el fin de generar un plan de seguridad que permita saber en cualquier momento el estado actual y cual es el paso a seguir para mantener el mejoramiento continuo, justificado y alineado con las metas del negocio.

[12] http://www.ca-systems.zetnet.co.uk/risk.htm
[13] http://www.cert.org/octave/
[14] http://csrc.nist.gov/mission.html
[15] http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF
[16] http://csrc.nist.gov/publications/drafts.html#sp80053

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6 REFERENCES

- Egevang, Kjeld and Francis, Paul, "RFC 1631 - The IP Network Address Translator (NAT)", Mayo de 1994, URL: **http://www.faqs.org/rfcs/rfc1631.html** (Agosto 5 de 2004)
- CERT, "CERT® Security Improvement Modules", Junio 19 de 2002, URL: http://www.cert.org/security-improvement/index.html (Julio 31 de 2004)
- Killalea, Toma, "RFC 3013 - Recommended Internet Service Provider Security Services and Procedures", Noviembre de 2000, URL: http://www.faqs.org/rfcs/rfc3013.html (Julio 31 de 2004)
- Bundesamt für Sicherheit in der Informationstechnik, "S 2.193 Establishment of a suitable organisational structure for IT security, from the German IT Baseline Protection Manual Standard security safeguards", Octubre de 2002, URL: http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/s/s2193.htm (Julio 31 de 2004)
- SANS, "The SANS Security Policy Project", URL: http://www.sans.org/resources/policies (Julio 31 de 2004)
- Defence Information Systems Agency, "DOMAIN NAME SYSTEM SECURITY TECHNICAL IMPLEMENTATION GUIDE", Version 2, Release 1, 19 de Marzo de 2004, URL: http://csrc.nist.gov/pcig/STIGs/DNS-STIG-V2R1A.pdf (Julio 31 de 2004)
- Microsoft Corporation, "How to Prevent DNS Cache Pollution", 10 de Octubre de 2002, URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;241352 (Agosto 5 de 2004)
- Barr, David, "RFC 1912 - Common DNS Operational and Configuration Errors", Febrero de 1996, URL: http://www.faqs.org/rfcs/rfc1912.html (Agosto 5 de 2004)
- Romao, Artur, "RFC 1713 - Tools for DNS debugging", Noviembre de 1994, URL: http://www.faqs.org/rfcs/rfc1713.html (Agosto 5 de 2004)
- Cisco Systems, "Configuring Port Security",URL: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800da706.html (Agosto 5 de 2004)
- Henderson, Scott, "CREATING A SPAMFILTER RELAY SERVER", 8 de Julio de 2004 http://www.geocities.com/scottlhenderson/spamfilter.html (Agosto 5 de 2004)
- C & A Systems Security Ltd, "COBRA Risk Consultant", 2002, URL: http://www.ca-systems.zetnet.co.uk/risk.htm (Julio 31 de 2004)
- CERT, "Octave", 26 de Agosto de 2003, URL: http://www.cert.org/octave (Julio 31 de 2004)
- National Institute of Standars and Technology, "Mission", 29 de Julio de 2004, URL: http://csrc.nist.gov/mission.html (Agosto 5 de 2004)
- National Institute of Standars and Technology, NIST Special Publication 800-18 "Guide for Developing Security Plans for Information Technology Systems", Diciembre de

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

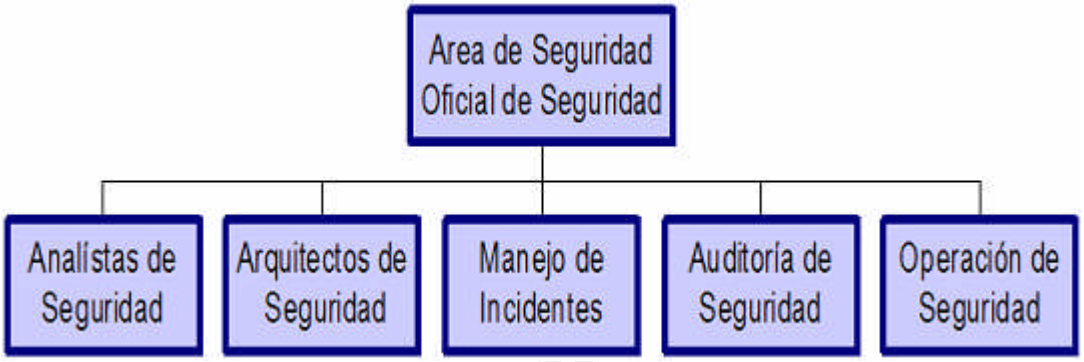
1998, URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF (Agosto 5 de 2004)

- National Institute of Standars and Technology, DRAFT NIST Special Publication 800-53 "Recommended Security Controls for Federal Information Systems", 31 de Octubre de 2003, URL: http://csrc.nist.gov/publications/drafts.html#sp80053 (Agosto 5 de 2004)

© SANS Institute 2004, Author retains full rights.

APÉNDICE A - CONFORMACIÓN DEL GRUPO DE SEGURIDAD

En la siguiente gráfica se puede ver la estructura establecida para llevar a cabo las labores de seguridad informática en el ISP. Inicialmente en cada uno de los grupos se tiene una persona, excepto el de manejo de incidentes y el de operación de seguridad, los cuales cuentan con dos, y debido a la carga que se ha tenido se está trabajando en solicitar una persona más. Esta estructura pretende separar los roles de diseño de seguridad, aseguramiento de equipos, operación de las herramientas de seguridad, atención a incidentes y auditoria, coordinados por el Oficial de Seguridad.



Gráfica 4

Es muy importante que el Oficial de Seguridad tenga contacto directo con la gerencia, con el fin de llevar a cabo un buen levantamiento de información que permita realizar un análisis de riesgos alineado con las metas; también es importante para la definición y establecimiento de políticas y procedimientos y su posterior auditoria.

A continuación se describen los roles y responsabilidades definidos dentro del área de seguridad.

Oficial de seguridad:

Encargado de velar por mantener el nivel de seguridad adecuado para la Gerencia.

Responsabilidades:

- Realizar periódicamente el análisis de riesgos
- Generar el plan de seguridad
- Definir los pasos a seguir para minimizar los riesgos
- Definir y mantener las políticas y procedimientos de la Gerencia
- Definir y mantener el Plan de Continuidad del Negocio (BCP)
- Definir y mantener el Plan de Recuperación ante Desastres (DRP)
- Reportar los resultados de las auditorias a la Gerencia
- Solicitar y justificar el presupuesto necesario para mejorar la seguridad
- Liderar los proyectos contratados para mejorar la seguridad
- Leer listas de correo y sitios de seguridad de los nuevos reportes de problemas descubiertos en Internet

Arquitectos de Seguridad:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Encargados de diseñar la arquitectura de seguridad de los servicios que presta la gerencia y de los nuevos proyectos.

Responsabilidades:

- Levantar la información de la arquitectura de seguridad de la Gerencia y los sistemas asociados
- Generar y actualizar de la documentación de la arquitectura del ISP
- Revisar el impacto de los nuevos equipos y servicios
- Diseñar la arquitectura de seguridad de los nuevos proyectos y de los cambios que se realicen a la arquitectura actual
- Diseñar la arquitectura de seguridad a los clientes con estos servicios
- Investigar y desarrollar nuevos productos y servicios de seguridad
- Evaluar y cuantificar los riesgos de seguridad de la Gerencia y de los clientes con servicios de seguridad
- Desarrollar las guías de aseguramiento para cada sistema
- Trabajar en conjunto con el Oficial de Seguridad para definir el DRP y BCP
- Trabajar en conjunto con el Oficial de Seguridad para definir los pasos a seguir para minimizar los riesgos
- Generar los planes de mitigación y contingencia para los riesgos que no puedan ser eliminados.
- Definir y mantener las políticas y procedimientos de la Gerencia
- Leer listas de correo y sitios de seguridad de los nuevos reportes de problemas descubiertos en Internet

Analistas de Seguridad:

Encargados de realizar el análisis y revisión del comportamiento de la Red y de los servicios que presta la Gerencia.

Responsabilidades:

- Corregir fallas de seguridad detectadas en los sistemas
- Revisar del comportamiento de red de la Gerencia, de los clientes y de los sistemas asociados, analizando los reportes de los diferentes sistemas de seguridad y de red (IDS, Firewall, Antivirus, Backup, IUM, MRTG)
- Realizar pruebas de vulnerabilidades y hacking ético a los equipos y servicios de la Gerencia, y de los clientes con servicios de seguridad
- Revisar nuevas vulnerabilidades y sus implicaciones en el nodo y en los clientes
- Generar alarmas de seguridad a las diferentes áreas reportando las vulnerabilidades encontradas
- Corregir las fallas de seguridad detectadas en los sistemas
- Analizar y asegurar los servidores y servicios de la Gerencia, y los nuevos equipos y servicios que se van a implementar
- Generar recomendaciones para los diferentes equipos de red, sistemas operacionales y servicios (“listas de chequeo”)
- Realizar la implementación de los nuevos proyectos
- Implementar las medidas definidas para minimizar los riesgos
- Leer listas de correo y sitios de seguridad de los nuevos reportes de problemas descubiertos en Internet

© SANS Institute 2004, Author retains full rights.

Manejo de Incidentes:

Encargados de Controlar y hacer seguimiento a los incidentes informáticos que se presentan desde y hacia los clientes del ISP.

Responsabilidades:

- Generar y mantener el grupo de respuesta ante incidentes del ISP
- Creación y actualización continua de la Políticas Aceptables de Uso del ISP
- Definir los procedimientos a seguir en caso de presentarse cualquier tipo de incidente
- Definir y entrenar al grupo interdisciplinario que participa en los procedimientos de respuesta ante incidentes
- Revisar e investigar los reportes de incidentes que llegan al ISP
- Generación de alarmas al grupo de arquitectos de seguridad de los problemas detectados en el ISP para definir su corrección
- Mantener actualizado el portal de seguridad del ISP
- Generar avisos a los clientes que están realizando ataques hacia Internet, seguimiento a estos casos y tomar las medidas correctivas de ser necesario
- Generar reportes de ataques informáticos realizados hacia la infraestructura del ISP
- Leer continuamente las listas de correo y sitios de seguridad de los nuevos reportes de problemas descubiertos en Internet y de las actividades anormales en Internet
- Generar alarmas a la Gerencia y a los clientes con servicios de seguridad, de los nuevos tipos de ataques y la forma de evitarlos o corregirlos
- Generar de documentos de recomendaciones para realizar instalaciones seguras de equipos, servidores y servicios
- Generar las estadísticas diarias de los incidentes presentados
- Leer listas de correo y sitios de seguridad de los nuevos reportes de problemas descubiertos en Internet

Auditoria de Seguridad:

Encargados de realizar una revisión continua del estado de la seguridad y detección de cambios no controlados en los equipos y servicios del ISP, generando los reportes y recomendaciones de mejoramiento.

Responsabilidades:

- Realizar en conjunto con el Oficial de Seguridad la definición y actualización de Políticas de seguridad
- Realizar auditorias periódicas de las Políticas de seguridad establecidas
- Generar reportes del cumplimiento de las políticas y medidas para mejorar
- Realizar auditoria de contraseñas de los equipos del nodo Internet (servidores, enrutadores, switches, CPE's)
- Realizar auditoria de equipos y servicios del ISP (pruebas de intrusión, hacking ético y de detección de vulnerabilidades)
- Generar reportes del estado de la red y de los diferentes sistemas auditados

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Realizar la definición y actualización de los procedimientos para la instalación de equipos y servicios
- Revisar y actualizar de las listas de chequeo para realizar las auditorias
- Revisar la inclusión de nuevos servidores y servicios
- Realizar en conjunto con el Oficial de Seguridad el Análisis de Riesgos
- Realizar auditoria de los sistemas de Seguridad (Firewall, Antivirus, Antispam, IDS, Backup)
- Leer listas de correo y sitios de seguridad de los nuevos reportes de problemas descubiertos en Internet

Operación de Seguridad:

Encargados de Operar, mantener y administrar los productos de seguridad del ISP

Responsabilidades:

- Administrar los servidores y equipos de seguridad (Firewall, Antivirus - Antispam, IDS, Backup)
- Implementar las solicitudes de modificaciones en los Firewall (nuevas políticas, cambios, eliminación)
- Implementar nuevas políticas de seguridad en los Detectores de Intrusos del ISP
- Implementar nuevas políticas de Backup para respaldar la información de los servidores
- Revisar logs y reportes de los productos de seguridad para verificar su correcto funcionamiento
- Generar reportes de funcionamiento de los productos de seguridad
- Generar alarmas en caso de que los productos de seguridad no estén funcionando de manera adecuada
- Generar alarmas en caso de que los productos de seguridad detecten algún comportamiento anormal
- Mantener el Inventario de Hardware, Software, Conexiones de red y de energía de los equipos del ISP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

APÉNDICE B – TABLA DE IDENTIFICACIÓN DE RECURSOS

En la siguiente tabla aparecen algunos de los recursos identificados dentro del levantamiento de información realizado con las diferentes áreas.

SERVICIO	IMPORTANCIA	RECURSOS	ACTIVOS
NAVEGACIÓN	ALTA	RED	TNT's
			Firewall
			CPE's Clientes
			Enrutadores ISP
			Switches ISP
			Canal Internacional
			Red Transmisión
		SERVIDORES	Autenticación
			DNS
			Directorio Activo
		FÍSICOS	Electricidad AC, DC
			Aire acondicionado
			Acceso
		HUMANO	Personas
GESTIÓN	ALTA	RED	CPE's Clientes
			Firewall
			Enrutadores Gestión
			Switches Gestión
		SERVIDORES	ISM
			Service Desk
			Activator
		FÍSICOS	Electricidad AC, DC
			Aire acondicionado
			Acceso
		HUMANO	Personas
CORREO	MEDIA	RED	TNT's
			Firewall

© SANS Institute 2004, Author retains full rights.

SERVICIO	IMPORTANCIA	RECURSOS	ACTIVOS
			CPE's Clientes
			Enrutadores ISP
			Switches ISP
			Canal Internacional
			Red Transmisión
		SERVIDORES/ SERVICIOS	Correo Front
			Correo Back
			Directorio Activo
		FÍSICOS	Electricidad AC, DC
			Aire acondicionado
			Acceso
		HUMANO	Personas
ALOJAMIENTO DE PÁGINAS	MEDIA	RED	TNT's
			Firewall
			CPE's Clientes
			Enrutadores ISP
			Switches ISP
			Canal Internacional
			Red Transmisión
		SERVIDORES	WEB
			SQL
			Directorio Activo
		FÍSICOS	Electricidad AC, DC
			Aire acondicionado
			Acceso
		HUMANO	Personas

© SANS Institute 2004, Author retains full rights.

APÉNDICE C – MATRIZ DE VALORACIÓN DE ACTIVOS

			IMPACTO SERVICIO				
ACTIVOS	VALOR	REDU	NAV	GES	COR	ALO	TOTAL
Personas	5	1	3	3	3	3	30
Servidores DNS	1	1	3	2	3	3	23
Control de Acceso	1	0	2	2	2	2	21
Servidores de Correo	2	1	3	1	3	3	21
Switches ISP	5	2	3	1	3	3	19
Firewall	2	2	3	2	3	3	19
Aire acondicionado	4	3	3	3	3	3	19
Enrutadores ISP	5	2	3	1	3	3	19
Electricidad AC, DC	3	3	3	3	3	3	18
Red Trasmisión	4	2	3	1	3	3	18
Enrutadores Gestión	2	0	1	3	1	1	18
Directorio Activo	1	1	3	0	3	2	15
TNT's	3	2	3	0	3	3	14
CPE's Clientes	1	0	3	1	0	0	13
Service Desk	2	0	0	3	0	0	11
Switches Gestión	2	0	0	3	0	0	11
Activator	1	0	1	1	1	1	11
Autenticación	1	1	3	0	3	0	11
Canal Internacional	5	3	3	0	3	3	11
Servidores ISM	1	0	0	3	0	0	10
Servidores WEB	2	1	1	0	0	3	6
Servidores SQL	2	1	1	0	0	3	6

Valor: Valor económico del activo en escala de 1 a 5.

REDU: Redundancia del sistema, calificada de 0 a 5, donde 0 significa que no tiene y 5 que garantiza 99,999% de disponibilidad

NAV: Impacto sobre el servicio de navegación. 0 ninguno, 1 bajo, 2 medio, 3 alto

GES: Impacto sobre el servicio de gestión. 0 ninguno, 1 bajo, 2 medio, 3 alto

COR: Impacto sobre el servicio de correo. 0 ninguno, 1 bajo, 2 medio, 3 alto

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ALO: Impacto sobre el servicio de alojamiento de páginas. 0 ninguno, 1 bajo, 2 medio, 3 alto

TOTAL: Valoración del activo con base en los parámetros anteriores. El valor se obtiene así: TOTAL = VALOR-REDU*5+C+I+A+NAV*3+GES*2+COR*2+ALO*2

Esta formula fue generada teniendo en cuenta la importancia de los diferentes servicios (alta=3, media=2, baja=1), definidas en columna importancia, de la tabla de identificación de recursos (apéndice B), disminuyendo el impacto de acuerdo con la disponibilidad de cada sistema y dándole un peso adicional si afectaban cualquiera de los principios de la seguridad: Confidencialidad, Integridad y Disponibilidad.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS