El Ciclo de Vida de la Seguridad

NIST - National Institute of Standards and Technology – U.S.

IDENTIFICAR: Conseguir el conocimiento y las capacidades organizativas necesarias para poder gestionar la ciberseguridad en la organización. Esta fase supone las bases para las demás.

• Desarrollo normativo, Plan Director y SGSI (Sistema de Gestión de la Seguridad de la Información)

• Definición de controles, indicadores y cuadros de mando

• Auditorías de cumplimiento

• Análisis y gestión de riesgos

PROTEGER: Implementar las contramedidas y salvaguardas que aseguren los servicios corporativos. Se trata de tener la capacidad de limitar o de contener el impacto de un suceso o evento de ciberseguridad.

• Asesoramiento en la incorporación de nuevas tecnologías

• Implantación de soluciones tecnológicas de Ciberseguridad

• Fabricación de soluciones y servicios propios

DETECTAR: Identificar la ocurrencia de un suceso o evento de ciberseguridad, a tiempo.

• Diagnósticos especializados (hackings, código fuente, etc)

• Gestión de vulnerabilidades

• Red team (equipo para simular un ataque dirigido)

• Infraestructuras de monitorización continua

• SOC´s (*Security Operation Center*)

RESPONDER: Medidas de actuación ante un suceso o evento de ciberseguridad para tratar de contener el impacto.

• CERT (*Computer Emergency Response Team*)

• SERVICIOS PROACTIVOS:

- Assessments

- Gestión de la configuración

- Inteligencia

• SERVICIOS REACTIVOS:

- Gestión de incidencias

- Análisis forense

RECUPERAR: Enfocado a la recuperación y resiliencia, minimizando el factor tiempo.

Definición y ejecución de:

• BIA (*Business Impact Analysis*)

• Plan de Continuidad de Negocio

• Pruebas

TAXONOMÍA DE ATAQUES CIBERNÉTICOS

Contenido abusivo

SPAM: correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.

Delito de odio: contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.

Pornografía infantil, contenido sexual o violento inadecuado: material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.

Contenido dañino

Sistema infectado: sistema infectado con malware. Ejemplo: sistema, computadora o teléfono móvil infectado con un rootkit.

Servidor C&C (Comando y Control): conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.

Distribución de malware: recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.

Configuración de malware: recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de web injects para troyano.

Malware dominio DGA: nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).

Obtención de información

Escaneo de redes (scanning): envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.

Análisis de paquetes (sniffing): observación y grabación del tráfico de redes.

Ingeniería social: recopilación de información personal sin el uso de la tecnología. Ejemplos: mentiras, trucos, sobornos, amenazas.

Intento de intrusión

Explotación de vulnerabilidades conocidas: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE - *Common Vulnerabilities and Exposures*). Ejemplos: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).

Intento de acceso con vulneración de credenciales: múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.

Ataque desconocido: ataque empleando exploit desconocido.

Intrusión

Compromiso de cuenta con privilegios: compromiso de un sistema en el que el atacante ha adquirido privilegios.

Compromiso de cuenta sin privilegios: compromiso de un sistema empleando cuentas sin privilegios.

Compromiso de aplicaciones: compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.

Robo: intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.

Disponibilidad

DoS (Denegación de Servicio): ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.

DDoS (Denegación Distribuida de Servicio): ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

Sabotaje: sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.

Interrupciones: interrupciones por causas externas. Ejemplo: desastre natural.

Compromiso de la información

Acceso no autorizado a información: acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.

Modificación no autorizada de información: modificación no autorizada de información. Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.

Pérdida de datos: pérdida de información. Ejemplos: pérdida por fallo de disco duro o robo físico.

Fraude

Uso no autorizado de recursos: uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales.

Derechos de autor: ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplos: Warez.

Suplantación: tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

Phishing: suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

Vulnerable

Criptografía débil: servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.

Amplificador DDoS: servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist.

Servicios con acceso potencial no deseado: servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.

Revelación de información: acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos: SNMP o Redis.

Sistema vulnerable: sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Otros

Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

APT: ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

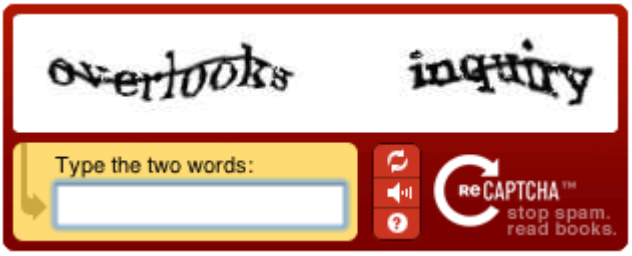
Ciberterrorismo: uso de redes o sistemas de información con fines de carácter terrorista.

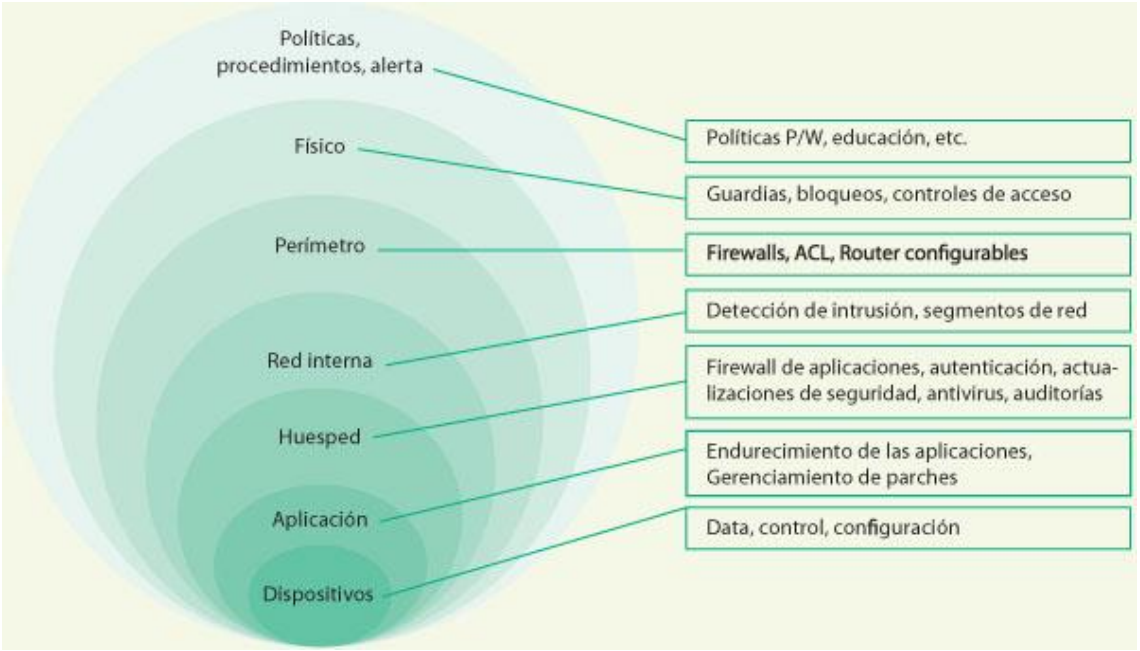
Daños informáticos PIC: borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial (INCIBE, 2021).

INFREASTRUCTURA DE DEFENSA - MECANISMOS DE SEGURIDAD

CAPTCHAs (*completely automated public turing tests to tell computers and humans apart*)

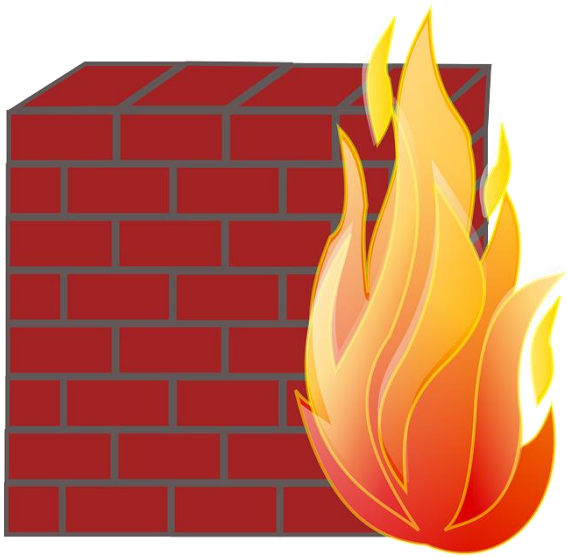
Prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos: Son pruebas desafío-respuesta controladas por que son utilizadas para determinar cuándo el usuario es un humano o un programa automático (bot)





Entre las técnicas de protección más utilizadas en redes destacamos los cortafuegos, sistemas de detección de intrusos, proxies, sistemas de gestión unificada de amenazas, VPN, sistemas centralizados de autenticación y zonas desmilitarizadas. Algunas ya se han estudiado en unidades anteriores, como los firewall, por lo que nos centraremos en cómo utilizarlas en redes, mientras que otras técnicas son nuevas y conviene conocerlas

Firewall (cortafuegos**)** [1]



Un firewall o cortafuegos es un dispositivo software o hardware que forma parte de un equipo o dispositivo de una red y está diseñado para proteger dicho sistema bloqueando accesos no autorizados y permitiendo solo los que deban ser permitidos cumpliendo con las directrices definidas en la política de seguridad de la organización.

Todos los mensajes que entren o salgan del equipo o la red pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Para permitir o denegar el tráfico, los cortafuegos suelen definir una política por defecto que se aplica sobre todos los paquetes que llegan a ellos.

Distinguimos dos tipos de políticas:

– **Políticas permisivas**: se deniega explícitamente el acceso a la red por parte de algunas aplicaciones, servicios, equipos o redes, permitiéndose el acceso al resto de aplicaciones. Esta política puede presentar problemas de seguridad porque cualquier aplicación no denegada explícitamente estará autorizada a acceder.

– **Políticas restrictivas**: por defecto está prohibido el acceso a los recursos del sistema, debiendo autorizarse de forma explícita y caso a caso. Esta política es la más adecuada para la mayoría de situaciones, porque si nos olvidamos de indicar alguna condición por defecto se rechazará su acceso, con lo que no constituirá un riesgo de seguridad.

Además de la política por defecto, la mayoría de cortafuegos definen reglas que son un conjunto de condiciones que deben cumplir los mensajes para que el firewall permita o rechace su paso.

Estas reglas suelen contener información como la siguiente:

– Equipo o red que ha enviado el mensaje.

[1] Los términos Firewall o cortafuegos en varios libros son utilizados para referirse al mismo dispositivo, por lo que en los materiales de lectura lo usaremos indistintamente.

– Dirección IP del equipo o red que recibirá el mensaje.

– Protocolo utilizado (TCP, UDP, ICMP).

– Puerto del equipo destinatario o emisor del mensaje.

– Acción a realizar sobre el paquete (aceptar, rechazar informando al emisor del motivo por el que se rechazó el mensaje, rechazar sin informar al origen, etc.). Si, por ejemplo, tenemos un servidor web, definiremos una regla para que acepte solo el tráfico que vaya al puerto 80 TCP, y otra para que se rechace el resto de tráfico que llega al equipo.

Algunos ejemplos de cortafuegos comerciales son: Agnitum Outpost Firewall, AnalogX PortBlocker, Ashampoo Firewall, Comodo Firewall, Droid- Wall, MailControl, Sunbelt Personal Firewall y Zone Alarm. La mayoría de estos programas suele ofrecer alguna versión gratuita con una funcionalidad reducida.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. Es necesario combinarlo con otros sistemas como herramientas antimalware, sistemas antispam, detectores/preventores de intrusos (IDS/IPS), proxies, etc.

Tipos de cortafuegos

Se puede clasificar los cortafuegos atendiendo a diferentes criterios, como su ubicación y su modo de funcionamiento:

Según el lugar en que se ubica el cortafuegos, podemos diferenciar entre:

– Cortafuegos de equipo o de host. Se instala en el equipo que se desea proteger. Analiza todo el tráfico que llega al equipo o sale de él y permite establecer qué aplicaciones pueden enviar y recibir información a través de la red.

– Cortafuegos de red o perimetrales. Este tipo de cortafuegos se ubica en un punto de entrada común a la red, como un router y actúa como barrera entre la red interna de nuestra casa u organización y la externa (Internet). Este tipo de cortafuegos se estudiará con más detalle en la unidad dedicada a la seguridad en redes.

Según su funcionamiento

Cortafuegos de filtrado de paquetes También llamados “cortafuegos sin estado”, filtran el tráfico mirando únicamente direcciones IP de origen y destino, puertos TCP/UDP o protocolo usado, pero sin llevar un seguimiento de conexiones o ver si forman parte de una secuencia anterior (estado). Este tipo de cortafuegos suelen permitir filtrados según campos de nivel de transporte, como el puerto origen y destino, o a nivel de enlace de datos como la dirección MAC.

Cortafuegos de aplicación Cortafuegos que actúan sobre la capa de aplicación del modelo OSI, con lo que pueden entender ciertas aplicaciones y protocolos. Permiten detectar si un protocolo no deseado se filtró a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Cortafuegos de estado Tienen en cuenta el estado de un paquete, esto es la colocación de cada paquete individual dentro de una serie de paquetes, ya que mantienen registros de todas las conexiones que les atraviesan y son capaces de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente o es un paquete erróneo. Este tipo de cortafuegos puede ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio. Un ejemplo de cortafuegos de estado es iptables (ESCRIVA, 2013).

Zonas desmilitarizadas

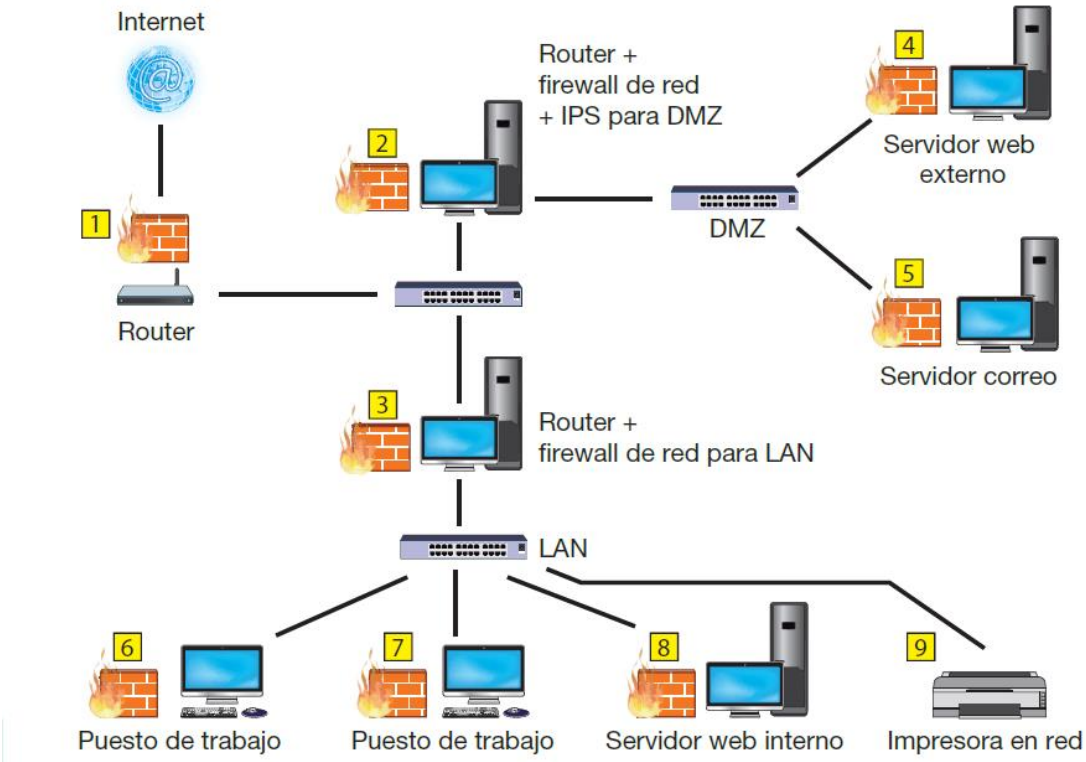


Fig. 7.36. *Despliegue completo de firewall en la empresa.*

(BUENDIA, 2013)

Una zona desmilitarizada o DMZ (DeMilitarized Zone, en inglés) es una red que suele albergar servidores que ofrecen algún servicio en Internet y que, generalmente, actúa como intermediaria entre la red interna de una empresa y la red externa, incrementando la seguridad de las redes internas. La red interna y la externa pueden establecer conexiones con la DMZ, pero desde la DMZ solo se permite establecer

conexiones con la red externa, denegando conexiones de entrada a la red interna. De esta forma, los equipos de la DMZ pueden iniciar conexiones con equipos externos de forma legítima como, por ejemplo, el servidor de antivirus corporativo que se descarga regularmente las firmas y actualizaciones de los virus.

Es importante remarcar que no se permiten conexiones desde la DMZ a la red interna porque se trata de una red con un nivel de seguridad relativamente bajo, con lo que podría darse el caso de que un atacante controlase alguno de los servidores que hay dentro de la DMZ y tratase de establecer conexiones con los equipos de la red interna.

Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

Detectores de intrusos - IDS

Este tipo de sistemas está formado por un dispositivo o software que monitoriza, alerta y/o elimina ataques a la red o a los equipos informáticos.

Dentro de este tipo de técnicas distinguimos entre sistemas detectores de intrusos y sistemas de prevención de intrusos:

– Sistemas detectores de intrusos, o IDS (Intrusion Detection System, en inglés), son un elemento pasivo que detecta ataques pero no los elimina.

Distinguimos tres tipos de IDS:

• **HIDS** (Host IDS), que monitoriza y protege un equipo.

• **NIDS** (Network IDS), que monitoriza y protege una red.

• **DIDS** (Distributed IDS), donde se dispone de NIDS distribuidos y gestionados por una consola.

– **Sistemas de prevención de intrusos o IPS** (*Intrusion Prevention System*, en inglés), son un elemento activo que trata de neutralizar el ataque, adaptándose a él. Suelen estar formados por un IDS y un cortafuegos que modifica sus reglas dinámicamente para evitar accesos no autorizados a la red.

El proceso utilizado para detectar ataques suele ser el estudio de la red en condiciones normales para elaborar estadísticas sobre el rendimiento y detectar anomalías.

Otra técnica utilizada para detectar ataques es similar a la utilizada por los antivirus para detectar infecciones de malware no recogido en su base de datos: se trata de “adivinar” si se produce un ataque mediante la comparación de patrones de ataques (firmas) con el tráfico que circula por la red en tiempo real.

Proxies

Un proxy o intermediario de red es un servicio, normalmente instalado en un servidor o dispositivo dedicado, que realiza la función de intermediario entre él y los clientes que solicitan un determinado servicio, como por ejemplo HTTP. Un proxy web por tanto es un dispositivo que trabaja en el nivel de aplicación de OSI.

El uso más habitual de un servidor proxy es permitir el acceso a Internet a los equipos de una organización cuando solo se puede disponer de un único equipo conectado, que es el propio proxy. Este permite a los clientes conectarse a una red (generalmente Internet) de forma indirecta a través de él, proporcionando de esta forma una capa adicional de seguridad. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado de la petición al cliente.

Algunas de las ventajas de usar un proxy son las siguientes:

– La navegación puede ser más rápida si se usa la caché y esta es suficientemente grande.

– Proporciona seguridad al proteger a los equipos cliente de la red externa.

– Posibilita definir filtros de contenidos y listas de control de acceso para permitir a las organizaciones realizar un control del servicio que se está usando.

Gestión unificada de amenazas

Los dispositivos conocidos como UTM (*Unified Threat Management*, en inglés) o gestión unificada de amenazas, combinan distintas técnicas de protección de redes como cortafuegos, antivirus, antispam, filtro de contenidos, detección y prevención de intrusos redes privadas virtuales y servidor proxy, todo ello en un único aparato.

Son la tendencia actual, sobre todo en pequeñas empresas, donde el ahorro de costes es crítico y no es posible invertir mucho dinero en soluciones de seguridad de varios fabricantes.

No obstante, hay que tener en cuenta que el hecho de que todos los sistemas de protección estén integrados en un solo dispositivo puede presentar problemas de rendimiento, escalabilidad y disponibilidad. Por ejemplo, un fallo completo en el dispositivo implica un fallo en todos los sistemas de protección de la red (ESCRIVA, 2013).

Spam

En las empresas, el correo electrónico es tan importante o más que el teléfono. Los empleados necesitan estar en contacto con otros empleados de la misma empresa, con los proveedores y con los clientes. Como responsables de la infraestructura informática, debemos garantizar que los mensajes se envían y reciben con normalidad, pero también que no hacemos perder el tiempo a nuestros usuarios entregando correos no deseados (spam).

Estos correos, como mínimo, llevan publicidad, pero también son una fuente de infección de virus y troyanos que pueden venir en un fichero adjunto o que aprovechan una vulnerabilidad del programa de correo.

Qué hace

El software antispam colabora con el servidor de correo para detectar mensajes indeseables.

Para determinar si un mensaje entra en esa categoría, el antispam utiliza:

- La cabecera del mensaje, buscando si el servidor de correo origen está en alguna lista negra de spammers reconocidos, si la fecha de envío utiliza un formato incorrecto (sugiere que el correo ha sido generado por un software de spam, no por un cliente de correo normal), etc.
- El contenido del mensaje, buscando palabras poco relacionadas con la actividad de la empresa (medicinas, etc.), mensajes cuya versión de texto plano es muy diferente de la versión HTML (sugiere de nuevo que ha sido generado con un programa de spam), etc.
- La propia experiencia del programa (autoaprendizaje), según el tipo de mensajes que maneja el servidor de correo de nuestra empresa en concreto.

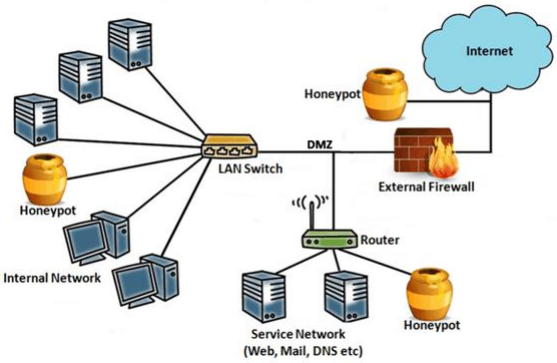
Cuando se detecta un correo spam, tenemos varias opciones:

- Bloquearlo aquí e impedir que llegue hasta el usuario; así le ahorramos molestias (leerlo, borrarlo) y evitamos potenciales infecciones. No se suele usar porque nunca tendremos la certeza de que no hemos eliminado algún correo importante.
- Dejarlo pasar, pero avisando al usuario de que es un correo sospechoso. Es la opción por defecto. El aviso al usuario consiste en añadir texto en el título del correo (por ejemplo, *** SPAM ***); esto le servirá al usuario para crear sus propios filtros en su programa de correo.
- Dejarlo pasar, pero convirtiendo el texto del correo en un fichero adjunto, para que sea más difícil engañar al usuario y solo lo abra si está seguro de que el correo le interesa.

LOS HONEYPOTS Y LAS HONEYNETS (SEÑUELOS)

Un honeypot es un servidor configurado y conectado a una red para que pueda ser sondeado, atacado e incluso comprometido por intrusos. Se trata, por lo tanto, de un equipo o sistema que actúa a modo de señuelo o trampa para los intrusos.

El concepto de sistema trampa ya fue propuesto hace algunos años por Cliff Stoll en su libro Cukoo's Egg. Por su parte, una honeynet (red señuelo) es una red completa que ha sido configurada y conectada a otras redes para que pueda ser sondeada, atacada e incluso comprometida por intrusos.



Los honeypots proporcionan varios mecanismos para la monitorización, registro y control de las acciones de los intrusos. De este modo, permiten analizar cómo los intrusos emplean sus técnicas y herramientas para intentar entrar en un sistema o en una red informática (cómo consiguen analizar y explotar sus vulnerabilidades) y comprometer su seguridad (cómo pueden alterar o destruir los datos, instalar programas dañinos o controlar de forma remota los equipos afectados). Además, estas actividades de monitorización y registro se realizan tratando de pasar de forma inadvertida para los intrusos.

Tal y como afirmaba el general chino Sun Tzu en su libro El Arte de la Guerra (siglo V A.C.), "lo que posibilita a un gobierno inteligente y a un mando militar sensato vencer a los demás y lograr triunfos extraordinarios es la información previa". Además, también en palabras de este famoso estratega, "la mejor forma de protegerse es saber cómo me van a atacar".

Por lo tanto, los honeypots y las honeynets entrarían dentro de las aplicaciones del tipo know your enemy ("conoce a tu enemigo"), que permiten aprender de las herramientas y técnicas de los intrusos para proteger mejor a los sistemas reales de producción, construyendo una base de datos de perfiles de atacantes y tipos de ataques. También podrían facilitar la captura de nuevos virus o códigos dañinos para su posterior estudio.

Así mismo, estos sistemas permiten desviar la atención del atacante de los verdaderos recursos valiosos de la red de la organización.

En cuanto al diseño de una honeynet, se han propuesto dos arquitecturas conocidas

como GenI (año 1999) y GenII (año 2002), siendo la segunda más fácil de implementar y más segura para la organización (VIEITES, 2014)

Referencias

BUENDIA, J. F. (2013). *Seguridad informática.* España: McGraw-Hill.

ESCRIVA, G. R. (2013). *Seguridad Informática.* España: Macmillan Iberia SA .

GMV SECTORES Ciberseguridad. (18 de 03 de 0221). Obtenido de GMV SECTORES Ciberseguridad

INCIBE. (18 de 03 de 2021). *INCIBE - Taxonomia*. Obtenido de https://www.incibe-cert.es/taxonomia

INCIBE-Riesgos. (18 de 03 de 2021). Obtenido de Analisis de Riesgos: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

STEWART, J. M. (2013). *Network Security, Firewalls and VPNs.* Jones & Bartlett Publishers.

VIEITES, Á. G. (2014). *Gestión de Incidentes de Seguridad Informática.* . RA-MA Editorial.