INTRODUCCIÓN

A lo largo de los últimos años, Internet ha tenido un crecimiento enorme, día a día encontramos un mayor número de sitios web, redes sociales (Facebook, Twitter, hi5, etc.), servicios de correo electrónico, sitios de comercio electrónico, transacciones en línea, y un sinfín de servicios, esto implica un mayor nivel de interacción entre los servicios ofrecidos y el usuario final. Uno de los principales servicios y de mayor uso dentro de internet es el correo electrónico, que ha tenido un considerable avance y hoy en día ha sustituido casi por completo al tradicional correo postal.

Uno de los principales problemas en el uso del correo electrónico es el spam, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, buscando principalmente que el consumidor adquiera algún producto o marca en específico, tales como artículos de salud o de aspectos finacieros, entre otros.

En el correo spam, usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, es más difícil localizar a los verdaderos remitentes, y no sirve de nada contestar a los mensajes de Spam: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos. Por ahora, el servicio de correo electrónico no puede identificar los mensajes de forma que se pueda discriminar la verdadera dirección de correo electrónico del remitente, de una falsa. Esta situación que puede resultar molesta en un primer momento, es semejante, por ejemplo, a la que ocurre con el correo postal ordinario: nada impide poner en una carta o postal una dirección de remitente aleatoria: el correo llegará en cualquier caso.

Además del *spam*, existen otros problemas que afectan a la seguridad y veracidad de este medio de comunicación:

- Los virus, que se propagan mediante archivos adjuntos infectando la computadora de quien los abre
- El phishing, que son correos fraudulentos que intentan conseguir, por lo regular, información bancaria

- Los engaños (*hoax*), que difunden noticias falsas masivamente
- Las cadenas de correo electrónico, que consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye a la propagación a gran escala del *spam* y de mensajes con virus, *phishing* y *hoax*.

Se debe poner especial atención en los mensajes que llegan a nuestra bandeja de correo electrónico, ya que la mayoría de éstos son correos que nosotros no solicitamos y es aquí cuando comienza el gran problema del spam, es importante no tomar atención a estos correos, ya que como se mencionó anteriormente también pueden ser trampas para descargar virus en nuestros equipos e infectarlos.

De esta forma, para combatir los peligros que pueden significar los correos basura, que generalmente contienen archivos adjuntos que son dañinos para los equipos o que apuntan al robo de datos privados, se idearon los programas antispam. Los mismos emplean distintas herramientas tecnológicas para eliminar estos riesgos.

El spam ya no se encuentra solamente ligado al e-mail o a Internet, sino que intenta llegar a la telefonía móvil, que sufre actualmente por medio de los mensajes sms y mms, y a la telefonía de voz sobre IP (VoIP). Dentro de Internet, podemos hallarlo también fuera de los correos electrónicos (en foros, redes sociales, etc.).

El objetivo de este informe es realizar la evaluación de las características de seguridad con que cuentan las principales herramientas antispam comerciales que existen hoy en dia en el mercado. Esto se realiza mediante el desarrollo e implementación de un laboratorio de pruebas. Compuesto por dos computadoras principalmente; un emisor, un destinatario de correo, y desde luego la herramienta antispam a evaluar. Desde este laboratorio fue donde se realizaron las pruebas de envío de diferentes tipos de correo electrónico (normal, con virus, con spam y

ambos), con la finalidad de probar la efectividad del filtro Antispam con el que cuentan estas herramientas.

Este informe consta de cuatro capítulos: En el primero se muestran una serie de antecedentes teóricos que son necesarios para el entendimiento posterior del informe. El segundo da una breve reseña de los proyectos realizados durante mi estancia en la Subdirección de la Seguridad de la Información UNAM/CERT. El tercer capítulo muestra de manera descriptiva todo lo realizado en este proyecto en específico, y un último capítulo que muestra los resultados generales de la evaluación de las herramientas, así como una comparativa de estos.

Objetivo

Evaluar soluciones antispam perimetrales mediante el desarrollo, instalación e implementación de un laboratorio de pruebas para llevar a cabo la metodología descrita, y finalmente generar un informe comparativo a fin de demostrar las fortalezas y debilidades de cada una.