Modelo de seguridad de la información en redes inalámbricas de tecnologías de la información para minimizar ataques de denegación de servicios

Paolo Cesar Ali Sánchez
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
paolokelpie3@gmail.com

***Resumen*—En la actualidad los ciberataques tienen lugar en cualquier lugar del mundo y afectan a todo tipo de infraestructuras. Todos los meses se reciben noticias de ciberataques que se llevan a cabo contra grandes empresas, gobiernos, universidades, comercios de Internet, entre otros, y ninguna de las soluciones comerciales disponibles parece capaz de ofrecer una solución al gran problema de la denegación de servicio. Es por ello que, con el objeto de ofrecer una adecuada orientación frente a dichas intrusiones, se plantea un modelo de seguridad de la información en redes inalámbricas de tecnologías de la información para minimizar los ataques de denegación de servicios.**

Palabras clave—Red inalámbrica, DDoS, UDP flood, ICMP flood, Syn flood, Connection flood, ISO 27001.

I. INTRODUCCIÓN

Desde hace años los ataques a las redes de internet, especialmente aquellos conocidos como DDoS (Distributed Denial of Service), han sido objeto de interés, tanto académico como profesional. Si bien este tipo de agresiones vienen produciéndose desde el origen de internet, al menos hasta la fecha no parecen existir soluciones eficientes que garanticen la detección, mitigación y comunicación de dichos ataques.

Conviene también destacar el elevado coste económico que este tipo de agresiones implican, así como la variedad de usuarios a los que puede ir dirigidos como, por ejemplo, comercios electrónicos que verán afectados sus servicios, proveedores de contenidos incapaces de entregar sus contenidos a los clientes o servidores que pierden la conexión con el exterior, entre otros muchos. Los aspectos mencionados, junto con otros, convierten a Internet en un ámbito inseguro en el que absolutamente ningún usuario se encuentra a salvo de este tipo de ataques y de sufrir sus consecuencias.

Esta necesidad de establecer y mantener transmisiones seguras usando canales de comunicaciones, como las redes inalámbricas ha conseguido que sea una tendencia y a su vez se ha convertido en algo extremadamente complejo, sobre todo para proteger la información contra los ataques de denegación de servicios.

Es por eso que en el presente artículo se plantea un modelo de seguridad de la información en redes inalámbricas de tecnologías de la información para minimizar los ataques de denegación de servicios, para el caso de estudio analizaremos los ataques que sufren las convertido instituciones públicas de Bolivia.

II. EL PROBLEMA DE LOS DDOS

Hoy en día, la información se maneja en grandes cantidades y de procedencias muy diversas, el valor añadido de una empresa puede ser la información que maneja. Como capital de la empresa cada vez es más importante mantener la seguridad de los datos e información, pero también los riesgos cada vez son mayores. Estos riesgos se pueden ser: errores involuntarios de personas y/o máquinas, desastres naturales, ataques voluntarios, siendo los ataques voluntarios los más comunes por la poca seguridad que existe en las redes y más en redes inalámbricas de las instituciones públicas.

Los problemas fundamentales que se tienen en cuenta en el riesgo de ataques voluntarios se clasifican en tres familias:

- Denegación de servicio: Disponibilidad, Prohibir el acceso a la información.
- Observación no autorizada: Confidencialidad, acceso a información por personas no autorizadas que pueden utilizarla para dañar la empresa.
- Modificación no autorizada: Integridad, acceso a la información y modificación, ya sea borrado, cambio, añadiendo o sustituyendo datos.

III. OBJETIVOS

El objetivo principal del modelo de seguridad de la información en redes inalámbricas es minimizar los ataques de denegación de servicios a los que está expuesto las diferentes redes de instituciones públicas y privadas.

Los objetivos específicos para el desarrollo del modelo son:

- Identificar los ataques de denegación de servicio que existen en la red inalámbrica mediante algunas herramientas de seguridad.

Para referenciar este artículo (IEEE):

[N] P. Ali, «Modelo de seguridad de la información en redes inalámbricas de tecnologías de la información para minimizar ataques de denegación de servicios», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 149-152, 2020.

- Estimar el estado actual de la seguridad en redes inalámbricas de tecnologías de la información.
- Elaborar un modelo de seguridad en redes inalámbricas tecnologías de la información.
- Validar los resultados después de la implementación y aplicación del modelo de seguridad de la información para redes inalámbricas de tecnologías de la información en relación a resultados anteriores de ataques de denegación de servicios.

IV. ESTADO DEL ARTE

A. *Principales incidentes en el mundo*

Durante las últimas décadas, diferentes avances técnicos produjeron grandes cambios en la tecnología de la información, la cual ha girado en torno a los datos y por ende a la información; su recopilación, almacenamiento, transmisión y presentación ha girado en torno a la tecnología de la información [1].

El informe de Verizon para su revista denominada Data Breach Investigations Report del año 2018, reporta a partir de la investigación de los incidentes contra la seguridad de la información, que la fuga de información en todo el mundo cae dentro de alguno de los siguientes patrones:

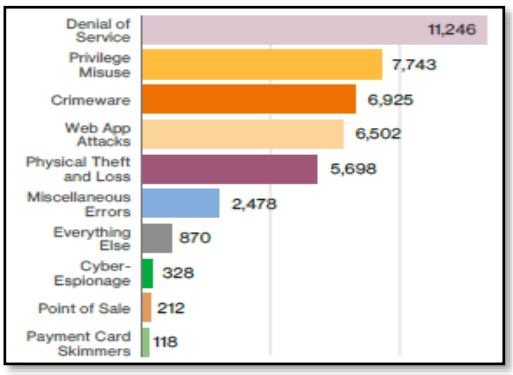

Fig. 1. Principales incidentes en el mundo [2]. Fuente: (Report, 2018)

Como se aprecia en la figura 1, los principales incidentes en el mundo son provocados por la denegación de servicios.

B. *Incidentes de seguridad en Bolivia*

El último informe al primer semestre de la gestión 2018 publicado por Centro de Gestión de Incidentes Informáticos (CGII) del Estado Plurinacional de Bolivia dependiente de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación AGETIC, despliega las estadísticas acerca de los incidentes de seguridad [3].

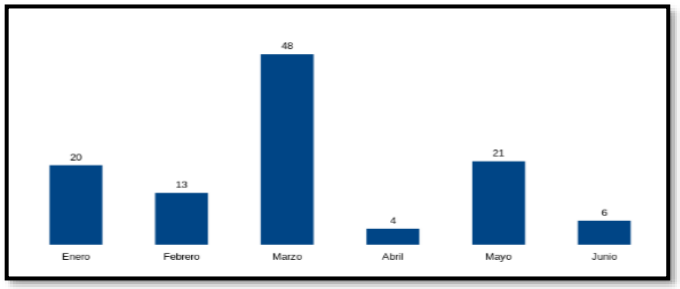

Fig. 2. Cantidad de Incidentes y vulnerabilidades atendidos primer semestre 2018. Fuente: (Centro de Gestión del Incidentes Informáticos, 2018)

La participación activa de profesionales en seguridad permitió identificar y solucionar vulnerabilidades a nivel de host y aplicación, así también la implementación de herramientas automáticas que realizan el monitoreo continuo de los servicios de instituciones del sector público. De los resultados predomina la configuración de seguridad incorrecta.

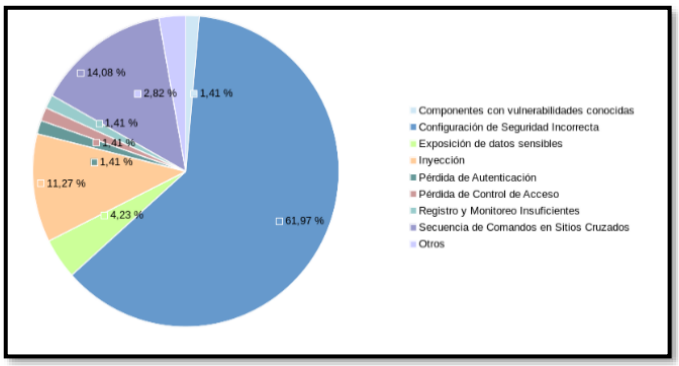

Fig. 3. Vulnerabilidades atendidas al primer semestre 2018. Fuente: (Centro de Gestión del Incidentes Informáticos, 2018)

Los incidentes con alto porcentaje de atención son las intrusiones que comprometen la seguridad de la información.

C. *Motivaciones de los Ataques DDoS*

Cabe mencionar que son muchas las causas que motivan la materialización de un ataque DDoS. Sin embargo, todos ellos cuentan con un objetivo común que consiste en la des habilitación de servicios brindados por los sistemas y aplicaciones expuestos en internet, de manera que el objetivo atacado no pueda continuar prestando el servicio para el que fue diseñado. En términos generales este tipo de ataques DDoS son llevados a cabo tanto por organizaciones distribuidas, entre las que se incluyen Anonymous u otras anónimas [4].

Estas compañías, organizaciones criminales, grupos de hacktivistas, organizaciones gubernamentales (NSA, MI5) y otros, llevan a cabo dichas agresiones con la finalidad de interrumpir el funcionamiento de infraestructuras web, centrales nucleares, centralitas telefónicas, servicios de pago, etc. [4]. La revista de seguridad de la Universidad Nacional Autónoma de México publico unas estadísticas de cuáles son las mayores motivaciones de ataques de denegación de servicios.

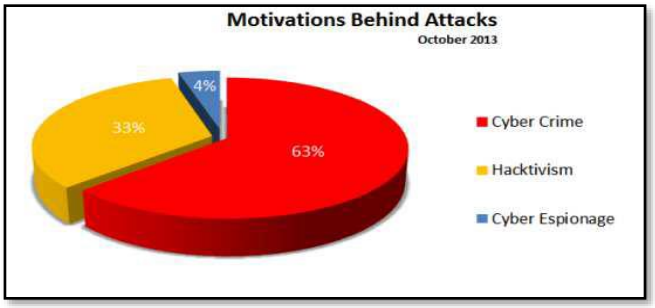

Fig. 4. Principales motivaciones de incidentes de DDoS. Fuente: (Seguridad en redes inalámbricas, 2018)

D. *Modelo de Seguridad de la información*

Un modelo de seguridad es la presentación formal de una política de seguridad. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada [5].

Un modelo de seguridad de la información es un diseño formal que promueve consistentes y efectivos mecanismos para la definición e implementación de controles [6].

De acuerdo a los autores López Barrientos y Quezada Reyes, los modelos se clasifican en:

- Abstracto: se ocupa de las entidades abstractas como sujetos y objetos.
- Concreto: traduce las entidades abstractas en entidades de un sistema real como procesos y archivos.

Además, los modelos sirven a tres propósitos en la seguridad informática:

- Provee un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas.
- Provee representación de política general de seguridad formal clara.
- Expresar la política exigida por un sistema de cómputo específico.

E. *Construcción de un modelo de Seguridad de la información*

Un adecuado modelo de seguridad está basado en políticas sólidas de seguridad de la información, teniendo como marco de referencia las mejores prácticas internacionales tales como ISO/IEC 27001 y ISO/IEC 27002, con el apoyo de la alta dirección y realizando una divulgación periódica y capacitación constante a los miembros de las organizaciones referente a los riesgos que se expone la información y los controles necesarios para su mitigación.

Se debe contar con herramientas de protección de última tecnología, permanentemente actualizadas, funcionando siete días a la semana, 24 horas al día y los 365 días del año (7x24x365) y con un alto grado de capacidad de respuesta, y un equipo de trabajo altamente calificado, que cuente con las certificaciones de seguridad informática necesarias, disponible 7x24x365, actualizado permanentemente y con un enfoque único y total en seguridad y administración del riesgo [7].

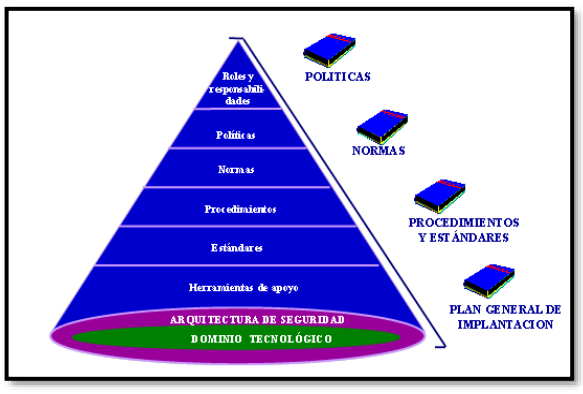

Fig. 5. Modelo de Seguridad. Fuente: (Nocella, 2013)

F. *Políticas de Seguridad*

Gómez, 2007 identifica exclusivamente para asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo permisos que se les dio. Por eso para a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión.
- Sensibilizar a los operadores con los problemas ligados con la seguridad.

G. *Normas ISO 27001*

La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia, subsistencia de las organizaciones. El hecho de disponer de la certificación según ISO 27001 ayuda a gestionar y proteger valiosos activos de información.

La norma ISO 27001 es un estándar internacional dedicado a la organización de la seguridad de las tecnologías de la información. Establece un sistema gerencial que permite minimizar el riesgo y proteger la información de amenazas externas o internas [8].

Actualmente es un estándar aceptado internacionalmente para la administración de la Seguridad de la Información y se aplica a todo tipo de organizaciones, independientemente de su tamaño o actividad.

Su objetivo principal es el establecimiento e implementación de un Sistema de Gestión de la Seguridad de la Información.

La seguridad de la información debe preservar la: *Disponibilidad*: Debe estar disponible cuando se necesita; *Confidencialidad*: La información sólo debe ser legible para los autorizados; *Integridad*: La información sólo puede ser modificada por quien está autorizado y de manera controlada; *Autenticación*: Verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice; *No repudio*: El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar la acción [9].

H. *Ataque de Denegación de Servicios (DDOS)*

DDoS o ataque distribuido de denegación de servicios consiste en un grupo de sistemas comprometidos (también conocidos como "ordenadores zombie") que atacan a un solo objetivo para causar una denegación de servicios a los usuarios que sí son legítimos [10].

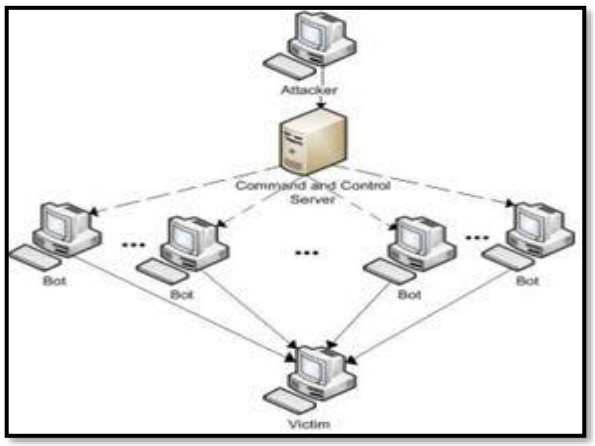

Fig. 6. Esquema de un ataque DDoS. Fuente: (UNAM, 2012)

Un sitio Web es como una puerta de acceso, sólo puede dar servicio a un número limitado de personas al mismo tiempo, por

tanto, si recibe más solicitudes de las que puede atender, el servicio se bloquea, nada entra ni sale.

I. Tipos de Ataque de DDoS

a) Syn Flood: Es el más común de todos, este ataque se basa en la esencia del protocolo de conexión TCP [11].

b) Connection Flood: La dificultad del servidor para atender un gran número de peticiones al mismo tiempo, si un atacante realiza 10,000 peticiones al servidor este estará ocupado por un período de tiempo, conforme caduquen las conexiones el atacante vuelve a establecer más conexiones impidiendo así que los clientes utilicen el servicio [11].

c) ICMP Flood: Este ataque también es conocido como "Ping-Pong", como una conversación por MSN donde los encargados contestan siempre a las personas que lo solicitan, entonces reciben un mensaje que dice: ¿estás? y responden: Sí, y les vuelven a decir ¿estás? y responden: Sí y así continúan por varios minutos [11].

d) UDP Flood: Este ataque utiliza el protocolo de conexión UDP para enviar una gran cantidad de paquetes al servidor utilizando muchas conexiones al mismo tiempo, ocasionando que los recursos (Memoria, Procesador) del servidor sean insuficientes para manipular y procesar la cantidad de información, en consecuencia, el sistema se bloquea [11].

V. ALTERNATIVA DE SOLUCIÓN

Existen múltiples modelos de prevención y contramedidas que tienen por objeto la mitigación de este tipo de ataques. En el caso que nos ocupa, con la finalidad poder enfocar las diferentes técnicas de mitigación, podemos basarnos en el modelo de Mirkovic [12].

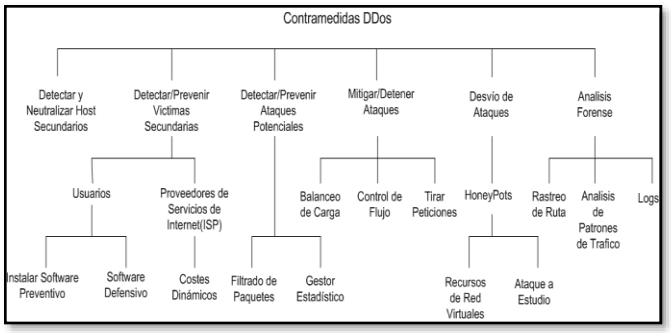

Fig. 7. Modelo de Mirkovic. Fuente: (Mirkovic & Reiher, 2004)

Este modelo clasifica en seis grupos las medidas y contramedidas a adoptar para prevenir los ataques. Entre ellas se incluyen las actuaciones para detección de hosts secundarios, para la detección de víctimas indirectas, para la prevención de potenciales ataques, para mitigación de los mismos, para su desvió y, finalmente, para su análisis forense. Esta clasificación constituye un modelo de referencia para detectar, analizar y resolver los problemas derivados de este tipo de ataques.

VI. CONCLUSIÓN

El presente artículo tiene por objeto introducir a cerca de un modelo de seguridad en redes inalámbricas para minimizar los ataques de denegación de servicios a instituciones públicas. Es una intención basada en el modelo de Mirkovic, compuesta por tres etapas de estudio: detección, comunicación y mitigación, que cooperan entre sí con la finalidad de ofrecer una adecuada protección frente al tan habitual problema de la denegación de servicio que tiene lugar en internet y que afecta a todo tipo de infraestructuras.

REFERENCIAS

[1] Druker, P. (1989). Book: The new realities. New York: Harper and Row.

[2] Report, 2. D. (2017, Julio 26). Verizon Media. Retrieved from https://www.verizondigitalmedia.com/es/blog/2017/07/2017-verizon-data-breach-investigations-report/

[3] Centro de Gestión del Incidentes Informáticos. (26 de Julio de 2018). Centro de Gestión del Incidentes Informáticos. Obtenido de https://www.cgii.gob.bo/es/noticias/estadistica-de-incidentes-de-seguridad-al-primer-semestre-2018

[4] Implementación de Seguridad En Redes Inalámbricas. México D.F.

[5] López Barrientos, M. J., & Quezada Reyes, C. (2012). Fundamentos de seguridad informática. México.

[6] Gómez Vieites, Á. (2007). Enciclopedia de la seguridad informática. México.

[7] Nocella, D. (24 de Febrero de 2013). Negocios & Management. Obtenido de http://negociosymanagement.com.ar/?p=2285

[8] ISO 27001, I. (2013). ISO/IEC 27001:2013.

[9] Santos, J. C. (2014). Seguridad y Alta Disponibilidad. España: RA-MA.

[10] UNAM, U. N. (2012). Ataque de DDOS. Seguridad TI.

[11] Caballero Gil, P. (1997). Seguridad Informática: Técnicas criptográficas. México: Ediciones Alfaomega.

[12] Mirkovic, J., & Reiher, P. (2004). A taxonomy of ddos attack and DDoS defense.

Breve CV del autor

Paolo Cesar Ali Sánchez es Licenciado en Informática por la Universidad Mayor de San Andrés (2011), Ingeniero de Sistemas por la Universidad Salesiana de Bolivia (2010). Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática UMSA.
Email: paolokelpie3@gmail.com