Resumen

En la actualidad, la sociedad depende cada vez más del Internet, por lo que es extremadamente importante para las empresas garantizar que este servicio esté disponible en todo momento, el proveedor de servicios de Internet, debe asegurar el acceso al Internet cumpla con una eficiente gestión en la seguridad de la información para proteger la red y sus datos, el aumento de los ciberataques y de los ataques de denegación de servicio distribuidos, los cuales son extremadamente disruptivos al punto que logran interrumpir o colapsar la red de la víctima. Por esta razón, es imprescindible desarrollar medidas de seguridad que estén a la par de cualquier ataque denegación de servicio distribuidos. El presente estudio utiliza varias herramientas de inteligencia de negocios las cuales permiten analizar los datos históricos, identificar, medir, supervisar, detectar y mitigar ataques denegación de servicio distribuidos en la infraestructura del ISP, con la finalidad de mejorar la toma de decisiones en seguridad de la información a través de un prototipo que muestre visualizaciones en Dashboard. Se propone una metodología de gestión de proyectos ágil Scrum, como fase de inicio se analiza la situación actual, para las fases del diseño, construcción y validación de la solución se basaran en el modelo de Ralph Kimball, para el análisis de situación actual del proveedor de servicios de Internet, los datos se obtienen de un controlador de software definido por red que analiza el tráfico en tiempo real, para la detección de ataques de denegación de servicio distribuidos, mediante algoritmos de aprendizaje automático de una máquina de vectores de soporte, el tráfico se clasifica en anómalo y normal, logrando evidenciar la mitigación de ataques denegación de servicio distribuidos y la importancia de la inteligencia de negocios como una herramienta crucial en la prevención y buenas prácticas de seguridad lógica en la red.

Palabras clave: inteligencia de negocios, denegación de servicios distribuidos, proveedor de servicios de internet, software definido por red, máquina de vectores de soporte.

Abstract

Nowadays, society has increased its dependence on the Internet. For companies is indispensable to maintain the high availability of service, in order that, the Internet service provider must make ensure of Internet access complies with efficient information security management to protect the network and its data. Am increase in cyberattacks and distributed denial of service attacks are extremely disruptive to the point that they manage to interrupt or collapse the network of victims. For this reason, it is essential to develop security measures that are on distributed denial of service attacks. This research uses several business intelligence tools which allow analyzing historical data, identifying, measuring, monitoring, detecting, and attacking distributed denial of service attacks on the ISP infrastructure, in order to improve decision-making in Internet security the information through a prototype that shows visualizations in Dashboard. An agile Scrum project management methodology is proposed, as the start phase the current situation is analyzed, for the design, construction and validation phases of the solution they will be based on the Ralph Kimball model, for the analysis of the current situation of the Internet service provider, the data is obtained from a software controller defined by network that analyzes the traffic in real time, for the detection of distributed denial of service attacks, by means of automatic learning algorithms of a support vector machine, the traffic is classified into abnormal and normal, managing to demonstrate the mitigation of distributed denial of service attacks and the importance of business intelligence as a crucial tool in the prevention and good logical security practices in the network.

Keywords: business intelligence, distributed denial of service, internet service provider, network-defined software, support vector machine.