Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions

Malik Qasaimeh, Rand Abu Hammour, Muneer Bani Yassein, Raad S. Al-Qassas, Juan Alfonso Lara Torralbo, David Lizcano

Revista: Journal of Software: Evolution and Process

Publicado: 08 August 2022

DOI: https://doi.org/10.1002/smr.2489

Resumen/Abstract:

Dado que el número de ciberataques a instituciones financieras ha aumentado en los últimos años, es esencial contar con un sistema avanzado que sea capaz de predecir el objetivo de un ataque. Un sistema de este tipo debe integrarse en los sistemas de detección existentes de las instituciones financieras, ya que les proporciona controles proactivos con los que detener un ataque mediante la predicción de patrones. Los sistemas de predicción avanzados también mejoran el diseño de software y las pruebas de seguridad de nuevas medidas avanzadas de ciberseguridad al proporcionar nuevos escenarios de prueba respaldados por la previsión de ataques. Este presente estudio desarrolló un modelo que pronostica futuros ciberataques basados en redes contra instituciones financieras utilizando una red neuronal profunda. El conjunto de datos que se utilizó para entrenar y probar el modelo consistió en algunos de los mayores ataques cibernéticos a instituciones bancarias en los últimos tres años. Esto proporcionó información sobre nuevos patrones que pueden terminar en un delito cibernético. Estos nuevos ataques también fueron evaluados para determinar similitudes de comportamiento con el ataque conocido más cercano o una combinación de varios ataques existentes. Luego se evaluó el desempeño del modelo de pronóstico en un entorno bancario real y proporcionó una precisión de pronóstico del 90,36%. Como tal, las instituciones financieras pueden utilizar el modelo de pronóstico propuesto para mejorar sus medidas de prueba de seguridad.

As the number of cyber-attacks on financial institutions has increased over the past few years, an advanced system that is capable of predicting the target of an attack is essential. Such a system needs to be integrated into the existing detection systems of financial institutions as it provides them with proactive controls with which to halt an attack by predicting patterns. Advanced prediction systems also enhance the software design and security testing of new advanced cyber-security measures by providing new testing scenarios supported by attack forecasting. This present study developed a model that forecasts future network-based cyber-attacks on financial institutions using a deep neural network. The dataset that was used to train and test the model consisted of some of the biggest cyber-attacks on banking institutions over the past three years. This provided insight into new patterns that may end with a cyber-crime. These new attacks were also evaluated to determine behavioral similarities with the nearest known attack or a combination of several existing attacks. The performance of the forecasting model was then evaluated in a real banking environment and provided a forecasting accuracy of 90.36%. As such, financial institutions can use the proposed forecasting model to improve their security testing measures.