Permasalahan Keamanan TI dan Penanganan Insiden Respon dalam Game *Online* Berdasarkan *Intrusion Detection System* (IDS)

Braham Lawas Lawu (23214319)
EL6115 –Operasi Keamanan dan Insiden Respon
Teknik Mikroelektronika, Program Studi Teknik Elektro
Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung

ABSTRAK

Permasalahan keamanan Teknologi Informasi (TI) sangatlah penting bagi penyedia layanan game, baik yang berbasis *offline* game maupun *online* game. Penyedia layanan game, khususnya game *online*, tidak menginginkan terjadi hal-hal yang tidak diinginkan dalam hal keamanan di dalam jaringannya maupun di dalam game itu sendiri. Untuk itu diperlukan pengetahuan yang baik dan juga informasi yang benar akan penanganan insiden respon, baik sebelum terjadinya serangan, maupun sesudah terjadinya serangan yang tidak diinginkan.

Penggunaan *Intrusion Detection System* (IDS) sebagai langkah dalam melakukan pengawasan, baik trafik dalam jaringan maupun kegiatan-kegiatan yang mencurigakan, dapat mengurangi aktivitas-aktivitas yang tidak diinginkan itu sendiri. Jika terjadi suatu aktivitas yang mencurigakan, maka IDS dapat memberikan peringatan ke dalam sistem atau *administrator* jaringan. IDS sendiri memiliki beberapa jenis dan pendekatan yang berbeda dalam mendeteksi suatu trafik. Secara umum, beberapa jenis IDS tersebut adalah: (1) IDS yang berbasis jaringan atau (NIDS), dimana IDS ini ditempatkan pada tempat strategis atau *node* penting dalam suatu jaringan untuk melakukan pengawasan trafik baik yang berasal maupun menuju kedalam perangkat di dalam suatu jaringan. Dan (2) IDS yang berbasis host (HIDS). IDS jenis ini bekerja pada *host* yang berdiri sendiri dalam sebuah jaringan. IDS ini melakukan pengawasan terhadap paket-paket yang berasal dari luar maupun dari dalam yang ditujukan pada satu *device* saja, kemudian memberikan peringatan kepada *user* atau *administrator* bahwa di dalam suatu jaringan terdapat aktivitas yang berpotensi sebagai serangan.

Inti pembahasan makalah ini adalah kajian mengenai permasalahan keamanan TI yang terjadi pada game *online* dan penanganannya berdasarkan model-model yang ada pada *Intrusion Detection* System (IDS). Dengan mengetahui permasalahan yang ada dan mengetahui penanganan insiden respon ini, diharapkan sistem keamanan dalam game *online* dapat dijaga.

Kata kunci : IDS, Insiden Respon, Keamanan Jaringan, Game *online*.

REFERENSI

[1] S. Ardi, and N. Shahmehri, "A Post-Mortem Incident Modeling Method", In *International Conference on Availability, Reliability and Security*, 2009.

[2] N. Hidayah, and R. Choo, "A Survey of Information Security Incident Handling in The Cloud", In *Computers & Securtty 49,45-69*, 2015.

[3] Zhonghua Zhang, Pin-Han Ho, Liwen He, "Measuring IDS-estimated Attack Impacts for Rational Incident Response: A Decision Theoretic Approach", In *Computers & Security 28, 605–614*, 2009.

[4] Donna D. Djordjevich, Patrick G. Xavier, Michael L. Bernard, Jonathan H. Whetzel, Matthew R. Glickman, and Stephen J. Verzi, "Preparing for the Aftermath: Using Emotional Agents in Game-Based Training for Disaster Response", In *IEEE Symposium on Computational Intelligence and Games (CIG'08)*, 2008.

[5] Saman A. Zonouz, H. Khurana, William H. Sanders, *Fellow*, *IEEE*, and M. Yardley, "RRE: A Game-Theoretic Intrusion Response and Recovery Engine", *IEEE Transactions On Parallel and Distributed Systems*, Vol. 25, No. 2, February 2014.

[6] Austin Silva, Glory Emmanuel, Jonathan T. McClain, Laura Matzen, and Chris Forsythe, "Measuring Expert and Novice Performance Within Computer Security Incident Response Teams", *Springer International Publishing Switzerland*, 2015.

[7] Stephen Mohr and Syed Rahman, "IT Security Issues Within The Video Game Industry", *International Journal of Computer Science & Information Technology (IJCSIT) Vol 3*, No 5, October 2011.

[8] Zachary O. Toups, Andruid Kerne, and William Hamilton, "Game Design Principles for Engaging Cooperative Play: Core Mechanics and Interfaces for Non-Mimetic Simulation of Fire Emergency Response", *Association for Computing Machinery, Inc., Sandbox, New Orleans, Louisiana, August 4 – 6,* 2009.