2019

Existing Evidence for the Effectiveness of IDS/IPS in Preventing Cyber Crime Incidents

David Maimon
Georgia State University, dmaimon@gsu.edu

Existing Evidence for the Effectiveness of IDS/IPS in Preventing Cyber Crime Incidents

David Maimon
Center for Evidence Based Cybersecurity
Georgia State University

An Intrusion Detection System (IDS) is a security device that monitors malicious activity against a computer network and applies specific detection techniques to determine attacks. In contrast, an IPS is a security device that monitors malicious activity and reacts in real-time by blocking a potential attack. In a similar vein to antivirus software, IDSs/IPSs use two detection techniques: misuse detection and anomaly detection. In effort to assess the potential effectiveness of IDS and IPS products in preventing the development and progression of cyber-dependent crimes we searched in six major academic search engines for studies published between the years 2000-2016 using experimental or quasi-experimental research designs.

We find that evaluations of IDS/IPS are usually performed by manual or automated testing of the device against data sets of sanitized real Internet traffic or actual Internet traffic generated from emulated user profiles, in order to assess the effectiveness of different features of the IDS/IPS. However, we could not find empirical research that assesses the effectiveness of IDS/IPS in preventing the development and progression of hacking incidents, malware infections, and DDoS attacks.