2019

Existing Evidence for the Effectiveness of Firewalls in Preventing Cyber Crime Incidents

David Maimon
Georgia State University, dmaimon@gsu.edu

Existing Evidence for the Effectiveness of Firewalls in Preventing Cyber Crime Incidents

David Maimon
Center for Evidence Based Cybersecurity
Georgia State University

A firewall is a network security component (either hardware or software) that is interposed between two computer networks in order to filter incoming and outgoing traffic between the two networks, according to a predetermined security policy and rules (Ioannidis et al 2000). Firewalls are configured with specific criteria to block or prevent unauthorized access, malware, and computer attacks on a network. In effort to assess the potential effectiveness of Firewall 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.

All in all, our search revealed that previous evaluations of firewall products include controlled lab experiments in which researchers simulated attacks and assessed different features of the firewall product, or automated penetration tests against tools that exploit security vulnerabilities. However, these tests fail to consider the behaviors of real attackers, and do not assess the effectiveness of this security tool in preventing the development of cyber-dependent crimes. Our search for empirical research that investigates the effectiveness of firewalls in preventing the development and progression of hacking incidents, malware infections, and DDoS attacks, and that matched the other criteria set for the search process, yielded no results.