2019

Existing Evidence for the Effectiveness of Prompt Vulnerability Patching in Preventing Cyber Crime Incidents

David Maimon

Existing Evidence for the Effectiveness of Prompt Vulnerability Patching in Preventing Cyber Crime Incidents

David Maimon
Center for Evidence Based Cybersecurity
Georgia State University

Software vulnerabilities (i.e. programing errors that could be exploited by online offenders) are commonly discovered and reported to the public on a daily basis. Once these vulnerabilities are discovered, their odds of being exploited as part of a cyber-dependent crime incident increase. Vulnerability patching involves the process of acquiring, testing, and installing security patches (i.e. a code change designed to update a computer program, in an effort to fix security-related defects) in order to keep computer security up-to-date. Failure to patch vulnerable systems may pose serious risks to a computer device, including unauthorized access and unavailability of system resources to legitimate users of the system. Thus, although security patch management may be a complex, expensive, and continuous process, it is necessary for improving the security of computer programs in large organizations. In effort to assess the potential effectiveness of prompt vulnerability patching 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.

Several empirical studies assess the probability of known vulnerabilities to be exploited in the wild; for instance, Nayak (2014) and associates predicted that only 15% of the known vulnerabilities in the most popular software products will ever be exploited. Moreover, Dacey (2003) estimated that effective patch management may prevent close to 95% of security breaches. However, we could not find any empirical research that assesses the effectiveness of prompt vulnerability patching 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.

References

Dacey, R. F. (2003). *Information security: effective patch management is critical to mitigating software vulnerabilities*. General Accounting Office.

Nayak, K., Marino, D., Efstathopoulos, P., & Dumitraş, T. (2014). Some vulnerabilities are different than others. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 426-446). Springer International Publishing.