Communications in Computer and Information Science

Privacy and legal implications regarding the processing of Honeypot Data

Pieterse, Heloise
Council for Scientific and Industrial Research (CSIR)
Meiring Naude Drive, Pretoria, 0184
Email: HPieterse@csir.co.za

Cyberattacks have been an ever-increasing threat against the cyber infrastructure of organisations. The act of exploiting known network vulnerabilities appears to be highly appealing to hackers where their potential payout is to find and collect valuable data housed by an organisation. To compensate for this matter, security teams can design and deploy highly advanced security tools to thwart cyberattacks, and one such tool is a honeypot. Honeypots possess the functionality of baiting intruders to interact with them whilst preventing said intruders from affecting real production and service systems. Ultimately, honeypots collect data associated with an intruder and the attack, which reveals valuable information that can be analysed and used to combat similar incidences. However, with the introduction of modern privacy laws, a number of consequences exist with the data honeypots collect. The paper will explore the limitations on processing honeypot data with the aid of related works published regarding honeypots, the POPI Act and the GDPR through literature revisions. Thus, this paper will discuss the privacy and legal implications that arise with processing data collected by a honeypot from the perspective of privacy laws established by both the European Union and the South African government.