Abstract

The large and open networks of Universities are particularly vulnerable because they often have multiple overlapping public and private networks. The staff, faculty members or students with infected devices might connect with the Universities networks. Many labs also have devices into their networks that were never intended to be there, which opens up new avenues of attack. This paper analyzed the security threats evolve specifically in University’s computing environment, and proposes risk management framework to guide security and risk executives through the process of network security management. The framework follows three phase activities: the first phase concentrates on the identification of the weak point in University’s networks; the second phase quantitatively measures the security risk level of
the University's networks; the third phase suggests plans for enhancing the security level of University's network environments. The proposed framework focuses on critical assets that are truly at risk.

References

- B. Dixon, "Understanding the FAIR Risk Assessment". Nebraska CERT Conference 2009.
- U. K. Singh and C. Joshi, "Quantitative Security Risk Evaluation using CVSS Metrics by Estimation of Frequency and Maturity of Exploit". The World Congress on
Managing Security Risks and Vulnerabilities in University's IT Threats Landscape

Engineering and Computer Science (WCECS 2016) San Francisco, USA.


Index Terms

Computer Science

Security

Keywords

Cvss; Security Risk; Security Threats; University Campus Network; Vulnerability