Als alle informatie telt : een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties

Hafkamp, W.H.M.

Publication date
2008

Bijlage 3 Summary

Over the last few years, the amount of time available to patch (fix) known security vulnerabilities in software has decreased tremendously. Time-to-patch is critical because nowadays the programs that take opportunity of software vulnerabilities (exploits) are available for download from the Internet within a few days after such vulnerabilities are discovered.
Large enterprises with complex IT infrastructures have usually organised IT service management according to an integrated process approach, which is often based on 'best practises' such as ITIL or standards such as ISO/IEC 20000 (Information technology – Service management). In such organisations, it is well understood that solid IT change management and related service management procedures are essential for complying with contractual service level agreements. However, enforcing these procedures could stand in the way of the quick responses that are required for effective IT security vulnerability and incident management.

This document contains the results of a study on IT security vulnerability and incident response processes in organizations with a standardized IT service management environment.

Chapter 1 gives an introduction of information security management practices, in particular the relationship with risk management and currently evolving attack trends.

Hypotheses, problem description and research goals and method are outlined in Chapter 2. The research question *'How do organizations respond to vulnerability and incident information when using formalized ITIL based management processes?'* is broken into four questions:
- How are 'IT security vulnerability' and 'IT security incident' defined?
- Which ITIL service management processes are essential to the research question?
- How do incident handling processes work within organizations?
- What are the goals and activities of Computer Security Incident Response Teams?

The chapter also describes the used research method, including the three Dutch case studies of ten banks, three university related computer security incident response teams and the team digital expertise of the national police.

Chapter 3 is titled 'Vulnerability and Incident Response State-of-the-Practise'. It starts with an overview of technical developments in firewall technology, intrusion detection and vulnerability scanning. The next paragraph deals with the standardization of IT service managements processes, in particular the ITIL framework, followed by a description of the evolution of incident response capabilities.

Chapter 4 describes the results from the casestudies. Among other things, the chapter contains descriptions of the organizations visited, an explanation of the operational frameworks used and statistics related to registered incidents.

Chapter 5 and 6 provide an analysis and conclusion based on the state-of-the-practise and the case study results. Four characteristics were analysed: size of the organization, type of service, response speed and knowledge. The main conclusion is that the vulnerability response capabilities of organizations with formalized ICT management processes are

rather poor, and that generic incident response processes are sufficient. However, incident response co-ordination for (cyber)crime-related incidents needs to be improved.

Finally, Chapter 7 describes an ideal model for IT security vulnerability and incident response management based upon the principles of standardized IT service management processes. Chapter 8 contains recommendations for further research.