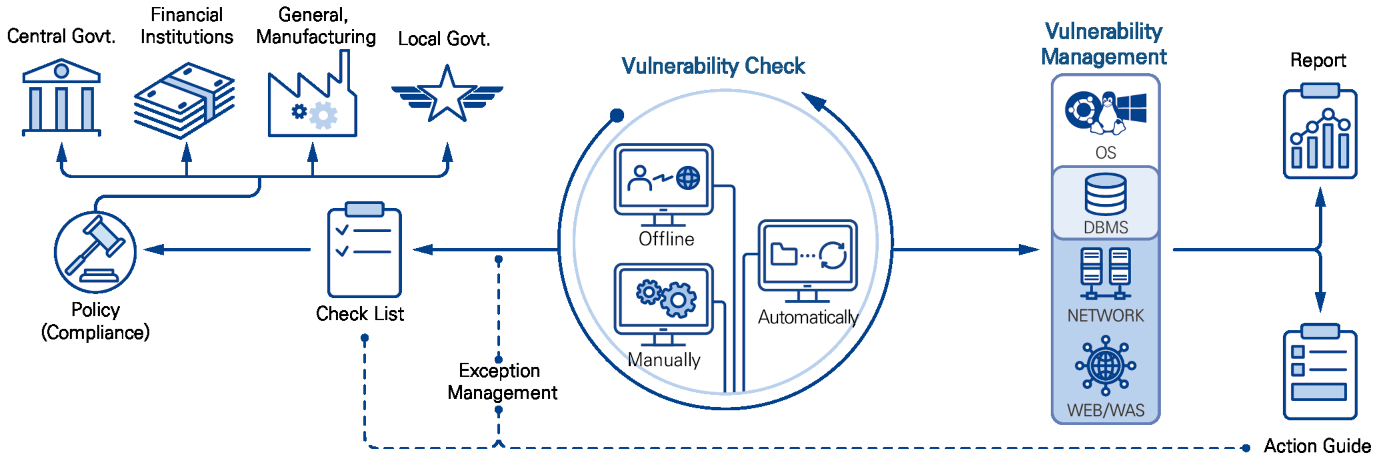
H www.lsware.com B blog.lsware.co.kr

Solutions for Diagnosing Security Vulnerabilities

SecuMS automatically checks for security vulnerabilities in infrastructure systems and provides solutions to problems found. In addition, it is the solution for diagnosing security vulnerabilities by collectively identifying the status of vulnerabilities and supporting monitoring at all times, which, in turn, helps clients to increase the security level.



Overview

Expansion of Vulnerability Management Scope

- Additional responses to vulnerability check items required by the supervisory authorities
- Increase of management systems such as OS, DBMS, WEB/WAS, and NW
- Continuous occurrence of new vulnerabilities

Increase in Internal and External Information Security Threats

- Increase in vulnerability incidents such as personal information divulgences
- The need for continuous management as well as response to security threats due to the increase in assets and vulnerabilities
- Security issues, such as HeartBleed of Open SSL, ransomware, and spear phishing

Heightened Need for Integrated Management

- Increased management scope due to various platforms and new versions
- Insufficiency of vulnerability check at all times and history management for IT infrastructure equipment
- Requirement by the supervisory authorities to “strengthen the financial IT autonomous system and regular monitoring system”

Needs for Compliance with Legal and Regulatory Requirements and Respond to Audits

- Expansion of vulnerability checks and security control to the extent of non-financial computer systems (Comprehensive measures to strengthen the security of financial computer systems)
- Checking technical vulnerabilities on a regular basis and taking actions against vulnerabilities found (ISMS, Information Security Management System)
- Annual vulnerability analysis and assessment on critical information and communications infrastructure

Expected Benefits from SecuMS

- Implementation of one-day security diagnosis system
- Improvements in the diagnosis process
- Indexing of IT security
- Security auditstable business management activities
- Making security practices a way of life

LSware Inc. 18th floor, Daeseong D-polis Building A, 606, Seobusaet-gil, Geumcheon-gu, Seoul, Republic of Korea, 08504
TEL +82-2-6919-0321 FAX +82-2-6919-0329

Key Features of SecuMS

Vulnerability Check

- Meeting Korean/international compliance standards
- Verificações de vulnerabilidade automatizadas regularmente
- Manual/Portable (Offline) Checks
- Support for user-defined (customized) scripts

Vulnerability Management

- Provision of vulnerability management processes
- Checking of what actions are taken and results from the actions taken against vulnerabilities
- Management of history for the actions taken
- Provision of history of inspections/checks
- Support for changing and setting vulnerability classes

Exception Management

- The setting of exceptions for diagnosis items
- Provision of exception status and history
- Application of individual/batch exceptions
- Re-detection when exception period expires

Report

- Provision of detailed reports
- Provision of daily reports on the status of vulnerabilities
- Provision of change in vulnerability trend and statistical data
- Provision of reports using reporting tools
- Provision of a feature to generate an own report from the targeted system when portable (Offline) inspections/checks are carried out

Advantages of SecuMS

Consulting

- Reflecting the checklist in compliance with industry-specific regulations (Finance, government, enterprises, local governments. institutions, etc.)
- Maintaining the existing Clienttele's security policies and updating mandatory policies
- Reflecting vulnerability inspections/checks standards of the Ministry of Science and ICT, the Financial Security Institute, etc.

Process

- Supporting the linkage with approval system, mail system, RMS, ESM, etc.
- Improving the work efficiency by systematizing the vulnerability diagnosis process
- Providing customized customer support through the customization

Safety

- Minimizing the system impact with resource control function
- Applying the mechanism to prevent server load and failure
- Proven stability in large infrastructure environments

Different

- Providing multi-scheduling function allowing the redundant settings
- Providing a function to manage the history of actions taken against vulnerabilities
- Supporting a function to set the exception period for vulnerability checks
- Providing detailed action guide in Korean

Mapping for Core Elements, Laws, and Guidelines

Core Elements	Key Certification Guidelines
Electronic Financial Transactions Act	• Article 21-3(Analyzing and Assessing Vulnerability of Electronic Financial Infrastructure) ①To ensure the security and reliability of electronic financial transactions, a financial company and an electronic financial business entity shall analyze and assess the following matters with respect to its or his/her electronic financial infrastructure and report the findings therefrom to the Financial Services Commission. 21-4 ② A financial company and an electronic financial business entity shall establish and implement a plan to take necessary complementary measures based on the findings from analysis and assessment of vulnerability in the electronic financial infrastructure under paragraph (1).
Comprehensive Measures to Reinforce Financial Institution's Data Security	• The vulnerability checks and complementary measures shall be thoroughly implemented under the responsibility of the CEO. • A system shall be established to ensure that complementary measures against vulnerabilities are thoroughly implemented, such as preparing implementation procedures corresponding to the findings of the vulnerability checks • The vulnerability checks and security control shall be expanded to the extent of non-financial computer systems • The security checks on internal business support systems, such as the website for education and PR, and the groupware, other than electronic financial infrastructure, shall be mandatory.
Protection Guidelines on Critical Information and Communications Infrastructure	• Article 13 (Analysis and Evaluation of Vulnerabilities) ① In accordance with Article 9 of the Act, when the head of the management organization has conducted the first vulnerability analysis and evaluation on the critical information and communications infrastructure under his/her jurisdiction he/she shall analyze and evaluate the vulnerabilities of critical information and communications infrastructure each year. ③ The head of the management organization shall establish and implement the plans necessary for the specific implementation of the vulnerability analysis and evaluation, such as the target, period, procedure, method, and budget formation and execution of vulnerability analysis and evaluation, in consideration of the criteria for the analysis and evaluation of vulnerabilities under Article 9 (4) of the Act.
Information Security Management System (ISMS)	• The certification system for the comprehensive management system, such as technical and physical protection measures established and operated to ensure the security of information and communications networks • Article 18-11 (Operational Security) In order to check whether the information system is exposed to known vulnerabilities, technical vulnerability checks shall be carried out regularly, and actions shall be taken against the identified vulnerabilities.

※ Relevant laws and regulations

Financial Services Commission "Electronic Financial Transactions Act", "Comprehensive Measures to Reinforce Financial Institution's Data Security"
Ministry of Science and ICT (Former Ministry of Science, ICT and Future Planning) "Protection Guidelines on Critical Information and Communications Infrastructure," "Notification on Information Security Management System Certification, etc."