Security LCM Services

YAMAKI Tsuyoshi, SHIBATA Akira, OHKOSHI Yoshihiko, KODAMA Jun

Abstract

Under the threat of cyberattacks that are transforming themselves on a daily basis, many enterprises are now becoming incapable of dealing with the prevailing conditions. This is because they are required to adopt appropriate routine operations for preventing cyberattacks at the same time as preparing responses to possible security incidents by introducing security systems. To respond to such needs, NEC has started "Security LCM Services" that provide reliable services from consulting to construction and operation, while targeting the continuous improvement of customer cybersecurity measures. This paper introduces the LCM Services Security features and discusses the effects of their introduction.

Keywords

security LCM, incident response, CSIRT, SIEM, cyberattack, consulting, assessment, forensics

1. Introduction

The need for cybersecurity has been increasing recently. Although interest in cyberattacks and illegal accesses has increased since the leak of personal information from the Japan Pension Service in 2015, countermeasures are not advancing satisfactorily. Therefore, cyberattack damage to various enterprises and organizations is still being reported. In December 2015, Japanese Ministry of Economy, Trade and Industry established the Cybersecurity Management Guidelines jointly with the Information Processing Promotion Agency, Japan (IPA). These guidelines clearly define cybersecurity as a management issue and the support of managers in promoting them was requested. Japanese enterprises are currently advancing their security measures by following these guidelines, but insufficiency or ineffectiveness in applying the suggested measures are tending to result in new issues. In this paper, we explain the issues that affect enterprises in coping with the rapidly increasing threats of cyberattacks and introduce the approach of NEC in dealing with them.

2. Issues Facing Enterprises

In our efforts to support the cybersecurity measures of our various customers, we have come to understand that they are troubled by common issues. These issues can be summarized in the following two ways.

(1) Lack of expert knowledge on security

Security measures can roughly be divided into pre-emptive measures for preventing security incidents and later measures that include actions to be taken subsequent to a security incident. The proactive measures cover a very wide range, from a system related matter which includes entrance/exit and endpoint monitoring, to an employee education support. A wide range of knowledge is required to comprehensively and effectively enforce such measures. Measures applied retroactively range from relatively established ones such as responses to computer or paper losses to those newly experienced by many enterprises, such as responses to targeted cyberattacks. Responses designed to deal effectively with the latter require very advanced, expert knowledge.

(2) Lack of security competent human resources

Many organizations have few human resources that feature a security handling capability, so that much of the relevant work is concentrated in the hands of these specialists. In such a situation, an organization's security measures cannot be expected to be advanced effectively. In fact, such organizations are unable to increase human resources because they are lacking in sufficient time and cost to support improvements.

The most realistic and effective means for dealing with these issues is to classify those that can be handled by one's own organization and those to be outsourced to an outside expert and to adopt the requisite actions appropriately.

3. Planning and Development of Security LCM

To help customers solve issues, NEC has systematized its knowledge of security technologies and measures developed since the late 1990's, as Security LCD for use via our outside-sales services.

LCM stands for Life Cycle Management. The Security LCM provides constant support for a security environment, from understanding current status and examining policy to operating the policy. Besides providing such support, it also observes threat that changes over time and then reviews the present status and re-examines the policy. NEC provides services for the optimum circulation of the Security LCM. Among these services, consultation, system construction and system operations are fields in which NEC's wide-ranging assets can be usefully demonstrated.

NEC has been committed to the security system development/construction and malware analysis domains since the 1990's. In the year 2000 and subsequently, the corporation has continued to accumulate more knowledge through the organization/operation of the CSIRT (Computer Security Incident Response Team) and analysis and incident response via "Code Red." We now possess an environment that fosters and retains a large number of advanced security engineers, thanks to our development and knowledge acquisition program, as discussed above.

Also, in the private enterprise area, advanced targeted attacks aiming at information theft and cybercriminal attacks aimed at theft of money, such as via ransomware attacks have recently been intensifying. To deal with these urgent issues, multilateral support solutions involving customer/staff promotions, planning of solution strategies, enforcement of assessments and incident response support are all required in order to enable the solution of issues that cannot be solved by only using tools such as entrance/exit measures and endpoint measures.

Our Security LCM based on NEC's advanced engineering group and our accumulated knowledge can provide comprehensive support for meeting these needs.

4. Overall Setting, Features of Security LCM

The overall setting of the Security LCM is as described below, where support services are provided for each of the phases that include; I) present status understanding and policy examination; II) architecture; III) operations (**Fig. 1**).

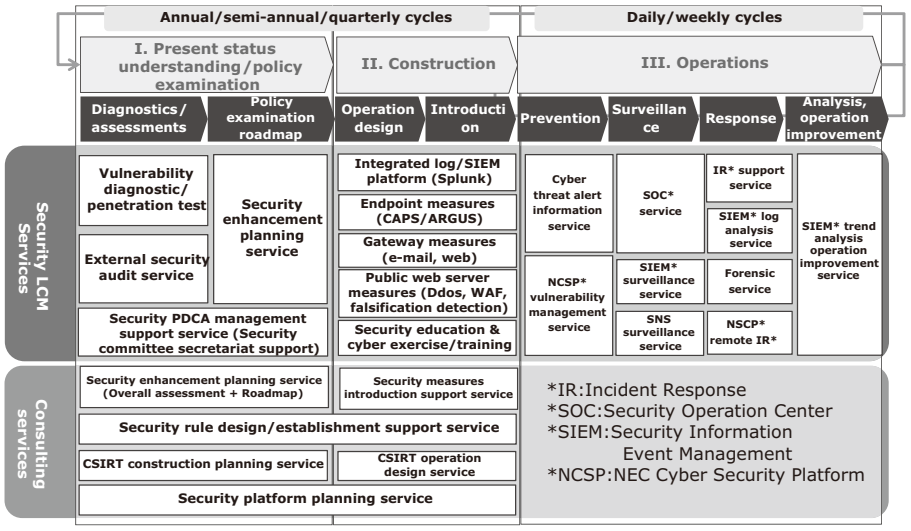

Fig. 1 Overall image of Security LCM.

"Phase I: Present status understanding/policy examination" includes the multilateral diagnoses and assessment service. This defines if the current security measures are adequate for the establishment of a security enhancement plan for filling the gap between the diagnosis/assessment results and the ideal situation.

"Phase II: Construction" includes the support service for security system construction and for the operational design of the provided security system with regard to its efficient operation.

"Phase III: Operations" includes the services for supporting the daily CSIRT operations such as those for incident detection and the one for receiving the advice and investigations of experts in the case of an incident. The features of the Security LCM are described in the following two subsections.

(1) Service provision applying NEC's knowledge

As NEC is engaged in the defence business, it adopts various, multi-layer security measures against the large number of cyberattacks that it receives each day. It has now been performing efficient operations for many years by promoting systematization and automation aimed at preserving the security of the entire NEC Group of more than 100,000 employees. The services introduced here apply the expertise that NEC has acquired via experience gained globally.

For example, NEC has built mechanisms that can visualize the status of security patch applications of all PCs in real time and those that can identify the signs of cyberattacks and attacked PCs from a huge volume of log data. These mechanisms are converted into templates that are incorporated into services wherever applicable.

(2) Flexible support meeting customer needs

Since the priority among the issues and threats to be dealt with tends to vary between customers, we can combine and provide the required services precisely according to each customer's situation and need. We are also able to provide continuous and overall support for customer security lifecycles.

For example, a customer who feels that the initial response and analysis of an incident poses a problem can instantaneously receive expert advice and investigation via the IR Support Service. A customer who wants to thoroughly review the current security system can receive reliable and continuous support via the services available from phases "I. Present status understanding/policy examination," "II. Construction" and "III. Operations."

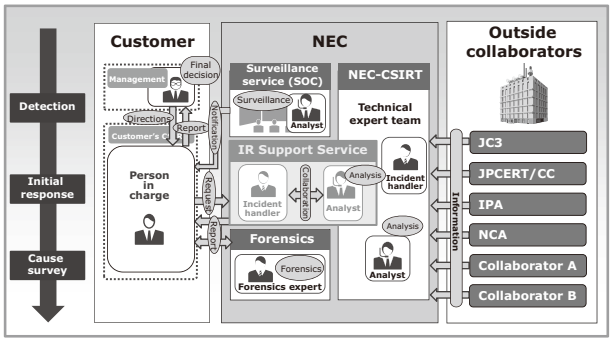

Fig. 2 IR Support Service.

5. Details and Features of the IR Support Service

This section describes the IR Support Service (**Fig. 2**), by which experts support an emergent response to a security incident. This service is regarded by many customers as being one of the most important issues faced by the Security LCM.

A security incident response needs a prompt initial response and appropriate action based on expert knowledge. When an incident occurs, the Security LCM Service accepts consultation via the information provision portal and adopts measures remotely, including offering advice on an initial response by a security engineer. Security engineers with experience in incident handling and malware analysis are pooled and provided in a shared manner to offer quick, practical support for responses to urgent security incidents.

For example, in case of any doubt with regard to a malware infection, this service not only performs a malware analysis for identifying the behavior of the malware but also gives in-depth advice covering incident response methods. This includes, how to identify the extent of damage by searching for a suspect infected terminal, based on the analysis results. Or on how to stop an illegal communication, if one is being generated. Such actions are often difficult to be taken by the customer enterprise itself. However, the security LCM service can take prompt actions based on experience because of the shared provision arrangement of the engineers who are able to handle multiple enterprises.

6. Future Perspectives of Security LCM

Cybersecurity is making progress on a daily basis. A new technology is probably being born even at this instant, just as a new threat is also being produced. Cybersecurity does not depend only on technology, it also requires management expertise including compe-

tent control. This field, which is very wide ranging is making rapid progress. NEC is resolutely creating high value services based on the fusion of technology and the knowledge that we have cultivated up to the present, by adopting the support of new technologies that are currently still at the R&D stage.

Authors' Profiles

YAMAKI Tsuyoshi
Senior Manager
Platform and Engineering Division

SHIBATA Akira
Assistant Manager
Platform and Engineering Division

OHKOSHI Yoshihiko
Platform and Engineering Division

KODAMA Jun
Platform and Engineering Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Remarks for Special Issue on Cybersecurity
Developing Fundamental Solutions to Combat the Rise in Cybercrime: What role can a third-party all-Japan industry-academia-government organization play in containing the threat posed by cybercrime?
Trends in Cybersecurity and NEC's Commitment to Developing Solutions

Social trends & NEC's approach
An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures
Latest Cyberattack Trends 2017 - Model Applying NEC Cyber Threat Intelligence -
The Measures Applied Internally by the NEC Group to Forestall and Prevent Cybersecurity Incidents

Cybersecurity solutions
Security Operations Center (SOC) and Security Monitoring Services to Fight Complexity and Spread of Cyber Threats
Incident Response Solution to Minimize Attack Damage
Enhancement of Incident Handling Capabilities by Cyber Exercise
Integrated Security Management/Response Solution – "NEC Cyber Security Platform"
Cloud-based File Encryption Service – ActSecure Cloud Secure File Service –
Security LCM Services
Secure Mobile Work Solutions That Exploit EMM
Cybersecurity Consulting Services in the World of IoT

Applications of AI technology to cybersecurity
Countermeasures against Unknown Cyberattacks Using AI
The Potential of AI to Propose Security Countermeasures
Detection, Auto Analysis of Cyber Threats Using Open Source Intelligence
Cyber-Physical Integrated Analysis Technology for Criminal Investigation Support

In-house efforts provide safety and security for customers
Efforts to Provide Safe, Secure Products and Services for Customers – Secure Developments/Operations –
Talent Management: Managing Cybersecurity Human Resources

Vol.12 No.2
January 2018

Special Issue TOP