Integrated Security Management/Response Solution – "NEC Cyber Security Platform"

ONODERA Hisato, YOSHIMOTO Masamichi, YAMAMOTO Kazuya

Abstract

Damage caused by cyberattacks targeting the information systems of enterprises and public institutions have recently become a significant social issue. In order to counter the increase in the number of attacks, Defense in depth combining several countermeasures are now required. Defense in depth is composed of proactive measures as well as of threat detection and post-incident measures. The proactive measures include vulnerability management procedures consisting of steps that include; the assessment of equipment configuration information, assessment of vulnerability information, investigations/risk analyses of vulnerabilities and the enforcement of countermeasures. This paper discusses issues posed by these steps and also introduces a solution applied by NEC called "NEC Cyber Security Platform."

Keywords

Count management, visualization, cyberattack, proactive measures, vulnerability management

1. Introduction

Following the recent increase in cyberattacks targeting the information systems of enterprises and public institutions, the motives of the attacks are shifting from acts undertaken to give pleasure to individuals to becoming commercial undertakings by professional criminals. Cases of damage caused by cyberattacks show no signs of declining. They recently include one in which illegal access to a server was made public and caused leaks of millions of items of customer information and one in which a virus infection of tens of thousands of workstations of a major overseas infrastructure business caused shutdown of its internal network.

Below, we introduce NEC's conceptual appraisal of the current trend in cyberattacks and discuss the measures being taken to deal with it.

2. Cyberattack Countermeasures

To counter the spread of attacks, it is required to adopt Defense in depth combining several countermeasures. Defense in depth is based on the idea that, even if a measure against an attack is broken, a subsequent measure will then be taken in order to prevent the attack succeeding. Individual technical measures that compose Defense in depth can roughly be divided into the following: "protective measures," "threat detection" and "post-incident measures."

(1) Proactive measures

Proactive measures are preventative measures for averting intrusions by attacks before they occur. They include the following: collection of vulnerability information for the application of security patches to equipment, restriction of administrative privileges to a required minimum number of users so that unauthorized users cannot access critical information, and application whitelisting so that only the permitted information may be accessed.

(2) Threat detection

Threat detection refers to finding a threat that has managed to intrude even though the proactive measure was provided. In order to detect intrusions of malware and successful attacks, it collects the logs of servers, terminals and network devices and the alert information of various security products, and

then checks if any suspicious communications exist or massive login failures by the administrator occur. In general, this operation is under the control of an organization called the security operations center.

(3) Post-incident measures

The post-incident measure refers to minimization of damage from an attack. An extension of the damage is prevented by identifying the scope of the effects and by adopting initial responses such as isolating terminals and changing the passwords. This action is followed by a full-scale response such as forensic and malware analyses for assessing an overview of damage and recovering from damage by clean installing any infected devices. In case an information leak is confirmed or a service provided by the company is affected, reporting or information disclosure outside of the company is performed as required.

3. Effects of Proactive Measures, NEC's Vulnerability Management

"Strategies to Mitigate Cyber Security Incidents"[1] proposed by Australian Signals Directorate (ASD) estimates that the defense of 85% of cyberattacks is possible by enforcing proactive measures. These include: "limitation of use of applications (application whitelisting)," "maintenance of applications at latest conditions (security patch application)" and "restriction of administrative privileges to a minimum."

As an actual example, WannaCry[2], ransomware that infected more than 300 thousand devices in 150 countries worldwide in May 2017, utilizes the vulnerability of the CVE-2017-0145, the patch for which was made public in March 2017[3]. Consequently, the potential damage of the ransomware was able to be avoided if the security patch was applied.

Among the measures proposed by the ASD, the process for applying security patch is regarded as being difficult to introduce and operate because it is evaluated as requiring high introduction and maintenance costs. On the other hand, in 2002 NEC started development of the Cyber Attack Protection System (CAPS) to protect the in-house information infrastructures and assets from cyberattacks. Patches were applied to 180,000 in-house units in order to maintain applications to be the latest conditions. Based on the Count management principle of "what is countable is manageable," CAPS visualizes risks and manages vulnerabilities by counting how many devices exist where and how many of them need to have measures applied. This strategy does not prevent attacks but it can succeed in significantly reducing the risks of attack damage. Below, we focus on the vulnerability management.

4. Processes and Issues of Vulnerability Management

Vulnerability management is generally performed via the following steps[4].

(1) Assessment of configuration information
(2) Assessment of vulnerability information
(3) Investigations and risk analyses of vulnerabilities
(4) Enforcement of countermeasures

The idea behind each step and the issues in the process of enforcement are as discussed below.

(1) Assessment of configuration information

This refers to identifying the number of devices in-house and collecting/managing the software configuration information of each of them. Collecting the configuration information enables a quick response in case a vulnerability is found.

The main issue in this process is the existence of a large number of management target devices, which tends to render the assessment of the software used by them and of their versions inadequate.

(2) Assessment of vulnerability information

This refers to the daily collection of vulnerability information published by the websites of OSs and software and by organizations issuing vulnerability information such as the IPA and JPCERT/CC. The obtained vulnerability information as well as the configuration information of the in-house systems are examined in detail for choosing essential information.

The main issue in this process is the long period taken for separating information related to one's own company from the published vulnerability information and the large amount of patch information provided by vendors.

(3) Investigations and risk analyses of vulnerabilities

This refers to selecting the high risk vulnerabilities from the collected information and collating them with the collected configuration information to check the effects on one's own company and in judging if countermeasures are required.

The main issue in this process is the impossibility of a quick response because of the long period taken for requesting investigations of the relevant departments and collating with the management ledger when investigating the effects on one's own company.

(4) Enforcement of countermeasures

Countermeasures such as applying patches and implementing workaround are planned and enforced for the vulnerabilities that are judged to require such measures. The security administrator monitors the countermeasure enforcement situation and confirms that the countermeasures are completed for all devices.

The main issue in this process is the huge costs required for enforcing the countermeasures using human labor. For example, assuming that there are 100 vulnerabilities in 10,000 devices, it would be required to enforce 1 million countermeasures and check the results, which is a hard task for human labor. In addition, errors in communications between departments would make it impossible to confirm the actual status.

5. "NEC Cyber Security Platform"

As mentioned above, NEC has been operating the CAPS for the vulnerability management. Since FY2016, the CAPS has been updated to the GCAPS (Global Cyber Attack Protection System), which is currently deployed throughout the entire NEC Group. The achievements of GCAPS in its in-house operations are used as the basis of commercialization for the NEC Cyber Security Platform (NCSP).

5.1 Functions and System Configurations of the NCSP

The NCSP is a solution that visualizes the situation of the countermeasures provided to the in-house device vulnerability and also offers support for their enforcement. It consists of the following components:

(1) NEC Security Intelligence
(2) NCSP Agent
(3) NCSP Manager

Fig. 1 shows the system configuration.

5.2 NEC Security Intelligence

The NEC Security Intelligence (hereinafter simply "Intelligence") supports assessment of vulnerability information.

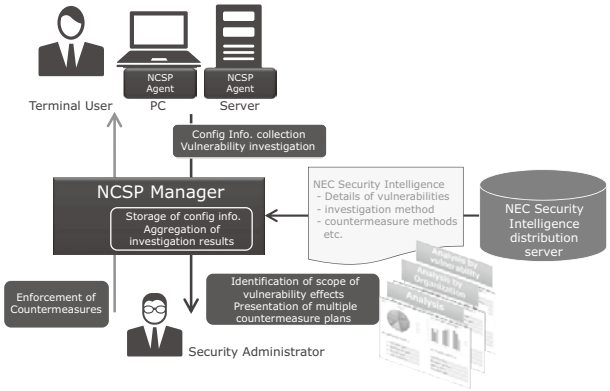

Fig. 1 System configuration of NCSP.

The "Intelligence" contains information including the search formulae for the vulnerability investigation by the NCSP and countermeasures, (patches, workaround, etc.). Every time an item of vulnerability information is published, NEC collects, evaluates and distributes it. The use of the "Intelligence" allows even people without advanced security skills to manage vulnerabilities at a similar level to NEC.

5.3 NCSP Agent

The NCSP Agent performs the configuration information assessment, vulnerability investigation and countermeasure enforcement in collaboration with the NCSP Manager. Elimination of human labor makes possible execution of the following processes quickly and at low cost.

(1) Assessment of configuration information
This process collects the device information (host names, OS names, CPU names, IP addresses, MAC addresses, installed software names, etc.) automatically.

(2) Assessment of vulnerability
This process receives the search formulae for vulnerability investigation from the NCSP Manager and investigates into the existence of vulnerabilities by checking the installed software versions, files and registries, etc. The results are sent to the NCSP Manager.

(3) Enforcement of countermeasures
When an automatic countermeasure instruction is received from the NCSP Manager, this process applies the countermeasure automatically. When a manual countermeasure instruction is received, it displays the risk viewer as shown in **Fig. 2**. The display urges the device user to enforce the countermeasure.

5.4 NCSP Manager

The NCSP Manager aggregates the configuration information collected by the NCSP Agent and investigates the results per organization to visualize the risks. **Fig. 3**

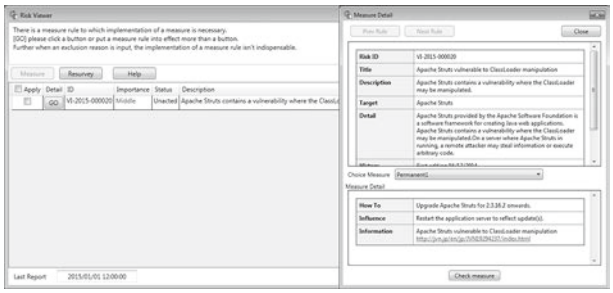

Fig. 2 Risk viewer (Left: List display, Right: Detail display).

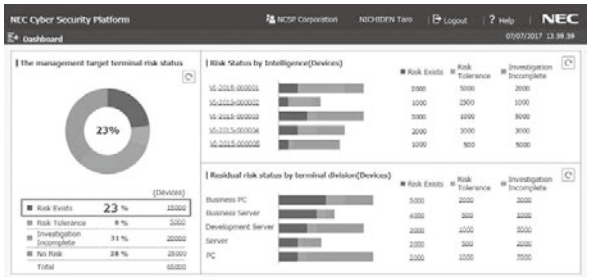

Fig. 3 Dashboard display of NCSP.

shows the dashboard display of the NCSP.

It supports the countermeasure planning of the security administrator by counting the overall risk situations of equipment as well as the number of devices under risk per vulnerability type, per organization and per terminal type. This allows the security manager to instruct and enforce countermeasures by considering the types of vulnerabilities and devices.

6. Conclusion

In the above, we discussed the implications of cyberattacks and the importance of vulnerability management in applying countermeasures and we also introduced NEC's NCSP solution. In the future, we are planning to enhance the incident response function in support of CSIRT operations.

* Apache Struts is a registered trademark or trademark of The Apache Software Foundation.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Reference

1) Australian Signals Directorate: Strategies to Mitigate Cyber Security Incidents
https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm
2) The White House: Press Daily Briefing by Press Secretary Sean Spicer -- #48, 2017.5.15
https://www.whitehouse.gov/the-press-office/2017/05/15/press-daily-briefing-press-secretary-sean-spicer-48
3) JPCERT/CC: Alert regarding ransomware "WannaCrypt," 2017.5
https://www.jpcert.or.jp/english/at/2017/at170020.html
4) Information-technology Promotion Agency, Japan (IPA): Vulnerability countermeasures guideline for the person in charge of information security (in Japanese), 2017.3
http://www.ipa.go.jp/files/000011568.pdf

Authors' Profiles

ONODERA Hisato
Assistant Manager
Smart Networks Division

YOSHIMOTO Masamichi
Manager
Smart Networks Division

YAMAMOTO Kazuya
Smart Networks 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 -

Vol.12 No.2
January 2018

Special Issue TOP