Approach to Cyber Security

Toru Harada Tsuneo Hamada

Information leaks from companies and organizations continue to occur as cyber attacks grow increasingly sophisticated. Amid the spreading damages, companies are required to be responsible for converting and improving from conventional information security such as virus and other malware (hereinafter referred to as virus) measures to “cyber security” that combats cyber attacks. This paper introduces OKI’s efforts related to cyber security, which is one of the most important tasks for companies, and the security solution that is provided based on OKI’s expertise.

Responding to Security Risks Surrounding Companies

In view of the increasing cyber attacks and the spread of damages, companies regard information security incidents as an important business risk that affects social credibility, damages brand image and ultimately ties to business downturn. Thus, they are embarking on developing and strengthening cyber security.

Japan’s Ministry of Economy, Trade and Industry, together with the Information-technology Promotion Agency, formulated the “Cybersecurity Management Guidelines” (December 2015) providing guidance for companies as they work to implement cyber security. In order to protect companies from cyber attacks, the guideline provides three principles for management to recognize the risks and promote cyber security under its leadership. The guideline also summarizes ten important instructions the management should give to their information security officer.

Preparing for a cyber attack by establishing an information security promotional system reflecting the intention of management is the first step in the response to security risks and an important issue for companies.

OKI’s Information Security Promotional System

Under the system centered on the “Information Security Committee (Chairperson: Chief Information Officer),” OKI promotes information security measures that meet security agency guidelines with three pillars of visualize, support and protect systems. The same measures (system, tools, education, etc.) are deployed to the entire OKI group through the information counter-leak manager appointed at each division and group companies. With this promotional system, information security is made uniform and measures strengthen in preparation for cyber attacks.

The specific contents of OKI’s three pillars are described below. The concept of the basic policy in information security is shown in **Figure 1**.

(1) Systems for visibility

- Understanding the use of information assets and implementation status of security measures to improve information security
- Monitor the usage of IT service to detect and prevent violations

(2) Systems for support

- Centrally manage confidential information, and protect the information through appropriate access authority and access logging
- Block information leak routes and prevent information leaks

(3) Systems for protection

- Define confidential information, determine concrete regulations of management process and make them known
- Carry out awareness activities such as information security training for all employees and blanket checks of information security

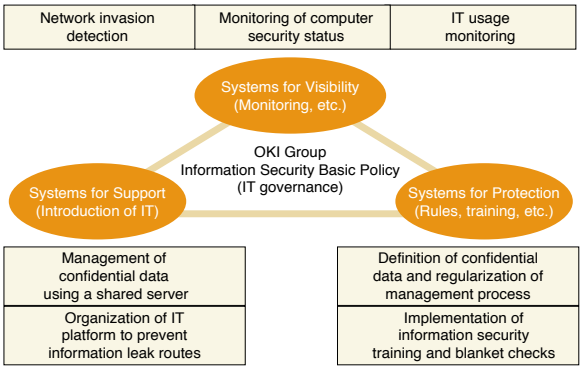

Figure 1. OKI Group Information Security Basic Policy

In addition to improving the mechanisms and system, information security promotion requires risk analysis from cyber attacks some of which includes daily occurring targeted/broadcasted email attacks, ransomware (files on PCs and servers are encrypted for ransom) and external vulnerability scanning. Staying tuned to external information such as security incidents in other parts of the world, vulnerability reports from security agencies and security guideline revisions is also necessary. Therefore, it is important to establish and operate the PDCA management cycle to improve and strengthen information security measures.

Measures against Cyber Attacks

What is important for cyber security is placing appropriate measures in the network, servers and PCs to protect information then monitoring the entire IT to quickly find the occurrence of problems, analyze the cause and swiftly take measures.

In order to properly take measures against cyber security, “inbound measures” for blocking unauthorized intrusions or downloads of viruses, “outbound measures” for blocking outflow of information should the server or PC be infected with a virus and “internal impropriety measures” for preventing illegal carry outs of customer information by monitoring file/database accesses must be effectively put in place. It is also important for these measures to be arranged in multiple layers. The reason being, even if an unknown virus breaks through the “inbound measures” and infects a PC on the company’s network, the “outbound measures” will block unauthorized server access preventing further infections and information leaks.

The representative mechanisms of inbound, outbound and internal impropriety measures implemented by OKI are introduced below. An outline of the cyber security measures is shown in **Figure 2**.

(1) Inbound measures

- Firewall: Block intrusions and DoS attacks from outside
- Intrusion detection/prevention: Detect unauthorized access (scanning activity, etc.) and block intrusions from outside
- Mail filter: Remove malware and dangerous attachments that maybe included with SPAM
- Behavior-based detection: Move suspicious file to a sandbox and from its behavior detect/block unknown virus that cannot be detected with antivirus software

(2) Outbound measures

- Firewall: Block unauthorized communication (e.g. virus communication) from inside the company
- IDS (Intrusion Detection System)/IPS (Intrusion Prevention system): Detect/block unauthorized access (e.g. virus communication) from inside the company
- Web filter: Block access by viruses to fraudulent servers from inside the company

(3) Internal impropriety measures

- Network connection control: Block network connection of unauthorized terminal through 802.1x authentication
- Integrated authentication: Prevent spoofing through Active Directory authentication
- DLP (Data Loss Prevention): Prevent information leak by restricting usage of portable storage medium and protection of confidential information
- DB monitoring: Prevent information leak by monitoring unauthorized access to the DB (illegal use of administrator authority, unauthorized operation, etc.)

(4) Other measures

- Antivirus: Detect and delete viruses
- Vulnerability diagnosis: Diagnose for potential vulnerability in server OS, middleware and Web applications
- Security incident measures: Prepare system and carry out training in response to incidents

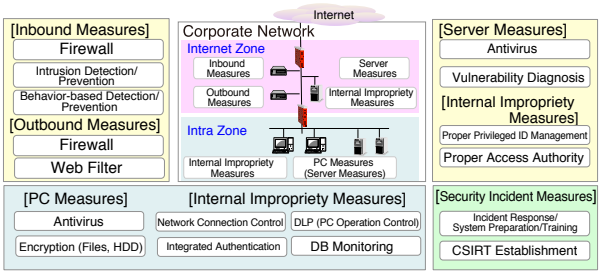

Figure 2. Cyber Security Concept

Preparation for Security Incidents

In preparation for security incidents, companies must establish an in-house CSIRT (Computer Security Incident Response Team), which responds to security problems on computers/networks (especially the Internet) and prevents the spread of damage.

Specifically, an emergency system including collaboration with internal and external organizations, standards for activating the emergency system, emergency workaround measures (e.g. preparing standards and methods for stopping the Internet) to prevent spread of damage, procedures for disclosing security incidents and the content must be determined.

In 2008, OKI established an in-house CSIRT, "OKI-CSIRT," and joined the Nippon CSIRT Association. The purpose was to improve incident resilience by "establishing a system that can respond promptly" when a security incident occurs and "information sharing and collaboration strengthening" with security agencies and other company CSIRTs.

In the eight years since OKI-CSIRT was established, OKI has responded to diversifying security risks through strengthening of information security monitoring (intrusions, virus infections, unknown virus invasions, information leaks to SNS, etc.), which is the basis of incident response, and mechanisms such as incident occurrence visualization developed from the monitoring results.

In addition, as an incident prevention activity, effort has been made to share internally the vulnerability information of software and network equipment as well as educating and raising awareness of employees.

An overall image of the OKI-CSIRT activities is shown in **Figure 3**.

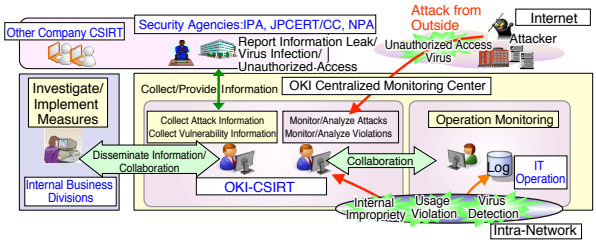

Figure 3. Overall OKI-CSIRT Activities

Security Solution Provided by OKI

Leveraging the expertise acquired in-house, OKI provides the Information Security Support Service. As shown in **Figure 4**, the service is a total solution ranging from "consulting," "vulnerability diagnosis," "CSIRT establishment/management," "education service" to "SOC (Security Operation Center) outsourcing."

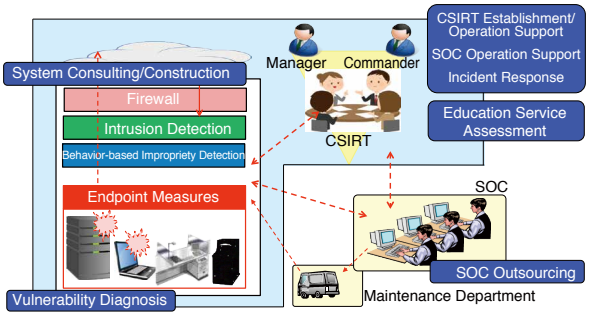

Figure 4. Information Security Support Service

The main services are described below.

- **Consulting**
  Support development of roadmap for governance planning and security strengthening as well as support security certification acquisition and system building/ improvement.
- **Vulnerability diagnosis**
  Analyze the current vulnerability state through the diagnosis of Web, network and mobile/wireless environment.
- **CSIRT establishment/operation**
  Support from concept planning to operation design of CSIRT security organization.
- **Education service**
  Support the development of human resources according to need such as latest trends in information security, incident cases/countermeasures, in-house rules, etc.
- **SOC Outsourcing**
  Respond to abnormal traffic and log analysis through remote monitoring from the security monitoring center. Also, support the improvement of security operations.

Information Security Support Service Provisioning Steps

The service is provided to customers in the following three steps.

1) **Consulting/Assessment**
   Visualize customer's current problems by investigating/ analyzing customer's current situation to extract problems and identify vulnerabilities

2) **Design/Construction**
   Based on the results of the analysis, study solutions such as reviewing system or architecture and support design/construction.

3) **Operation/Maintenance**
   Support daily monitoring/analysis and incident investigation/response either remotely or on-site.

Enhanced Security through Support Cycle

Cyber attacks evolve day by day, thus continuously turning the information security support cycle shown in **Figure 5** is vital to minimizing security risks. OKI's Information Security Support Service realizes continuous security enhancement by providing service to all phases from consulting to building and operations support.

Figure 5. Information Security Support Cycle

Realization of an Efficient Support Cycle

In order to counter the daily evolving threat, it is necessary to turn the information security support cycle continually and more efficiently. Analyzing the logs scattered in the internal system and finding improvement points in information security is an effective method. How the log analysis is conducted will be the key to the realization of an efficient support cycle, and the solution for this is an integrated log management system called SIEM (Security Information and Event Management). OKI's Information Security Support Service recommends the implementation of SIEM, and it is introduced below.

Through the collection and central management of multiple security devices, databases, application logs and events, SIEM enables event log visualization, correlation analysis and early threat detection/response. **Figure 6** shows the effect before and after the implementation of SIEM.

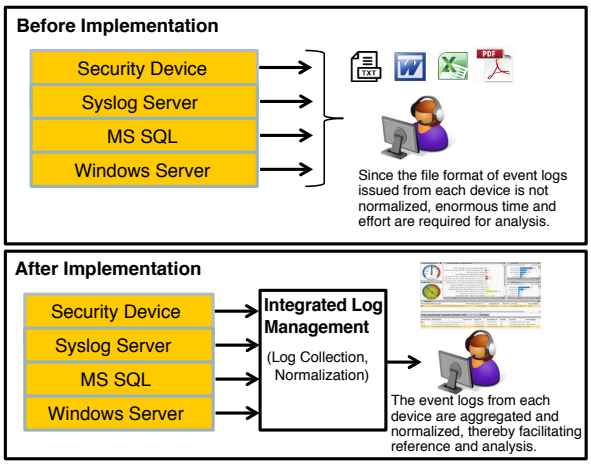

Figure 6. Effect of SIEM Implementation

The merits after SIEM implementation are summarized below.

- **Improved convenience**
  Aggregation and normalization of event logs from multiple devices makes it easier for administrators to perform reference and analysis.
- **Improved security**
  Constant monitoring of the centrally managed event logs enables early detection of incidents such as unauthorized access and abnormal operations and makes it possible to deal with the problem promptly.
- **Reduced operation man-hour/cost**
  Since visualization and correlation analysis are always performed on the event log, time and man-hour spent to complete the analysis are reduced.

Response to IoT Security

As use of IoT spreads in the coming years, various objects (devices) will be connected to the Internet. Understandably, these devices will be targets of cyber attacks. In response to the new threats brought on by IoT, Japan's Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry formulated the "IoT Security Guidelines" (July 2016) that presents security guidelines for providing IoT equipment, systems and services.

OKI regards IoT security as an important issue. Therefore, OKI is evaluating and studying the implementation of technologies and products, some of which includes AI, edge, IoT and next generation endpoint security, to realize efficient analysis of enormous logs accompanying the increase in network connected devices and to ensure secure connection of wide variety of devices such as factory manufacturing equipment and sensors.

Conclusion

This article introduced OKI's in-house cyber security efforts and the security solution it can provide to customers. Making use of the expertise gained in-house, OKI will deploy its security solution, the Information Security Support Service, and continue to meet the challenges of providing customers with safe and secure information communication systems including IoT. ◆◆

Authors

Toru Harada, Information Planning Division, Information & Technologies Planning Group

Tsuneo Hamada, Business Development Division, ICT Business Division