Critical Information Infrastructures Management System and Security Issues

Focusing on the Public Administrative Sector

Jun Heo
Internet Service Protection Team
Korea Internet & Security Agency
Seoul, Korea
herjune@kisa.or.kr

Wan Suk Yi
Internet Service Protection Team
Korea Internet & Security Agency
Seoul, Korea
wsyi@kisa.or.kr

***Abstract*— With Korea's transition to an advanced IT nation, its key infrastructures, including administration, transportation, healthcare, finance and communications, have become absolutely reliant on IT systems. This research examines systems in place in Korea for defense against cyber hacking and electronic invasions, and internal and external threats to the critical information infrastructure of the administrative sector, in which critical administrative service is provided to Koreans through e-government, and technical, physical and managerial measures to combat such threats are discussed.**

Keyword - Security; threats; administrative sector.

I. Introduction

The IT society is absolutely reliant on communications infrastructure. Social infrastructures, including administration, transportation, healthcare and education, rely on the communications infrastructure to function. A breakdown of the communications infrastructure due to destruction or malfunction will result in other social infrastructures malfunctioning. Thus it can be said that the information infrastructure is the core infrastructure of an IT society.

The Korean government implemented the revised Communications Infrastructure Protection Act in 2001 to systematically protect critical communications infrastructures in the finance, communications and energy sectors. To combat the increasing losses occurring from a rapid advancement of techniques used in electronic invasion activities, including the distribution of malicious programs, the Communications Infrastructure Protection Act stipulates preventative measures, countermeasures and recovery measures for systematic designation and protection of critical information infrastructures [1].

The communications infrastructures are designated as critical information infrastructures in accordance with 5 standards stipulated by the Communications Infrastructure Protection Act. Once designated as a critical information infrastructure, a risk assessment must be performed within 6 months. Subsequently, risks assessments are carried out once every 2 years. Based on the outcome of the risk assessment, the manager of a critical information infrastructure must implement short or long-term measures as required. Such measures are incorporated in the protection policies for the following year to achieve effective protection of critical information infrastructures. Also, protection policies are reviewed in the following year to verify that various protective measures have been taken as planned. Through such a process, critical information infrastructures are systematically protected [2].

As the social infrastructures in Korea, such as administration, transportation, healthcare and finance, are absolutely reliant on IT systems, efforts are being made to continuously expand the communications infrastructure. Since 2009, additional critical information infrastructures have been designated in the administrative sector.

A wide range of civil services are being provided in the administrative sector with ongoing e-government support. As the administrative sector is closely linked to the administrative bodies of cities, counties and districts throughout Korea, security breach in the administrative sector is highly likely to escalate to a national scale.

This research examines critical information infrastructure policies and their management systems. Also, threats to public service systems in the administrative sector being designated as critical information infrastructures, such as the e-government, and their protective measures are examined to provide reliable data for utilization in public administration.

II. Critical Information Infrastructure Policies and Management System

Communications infrastructures are managed under the jurisdiction of central administrative agencies. In order to provide systematic and comprehensive governmental protection of critical information infrastructures from electronic invasions, the Communications Infrastructure Protection Act stipulates the operation of the Communications Infrastructure Protection Committee to oversee the formation and execution of communications infrastructure protection policies to achieve cooperation on prevention and management of security breaches by various central administrative agencies.

Duties of the Communications Infrastructure Protection Committee include mediation in critical information infrastructure protection policies; review of formation and execution of protection plans; and review of systemic improvements and policies related to the protection of critical information infrastructures.

The Communications Infrastructure Protection Activities Committee was established to support the operation of the Communications Infrastructure Protection Committee by reviewing matters presented to the Communications Infrastructure Protection Committee or as directed by the chairman of the Communications Infrastructure Protection Committee.

In the event of a serious security breach in a critical information infrastructure, the Communications Infrastructure Protection Activities Committee operates a temporary security breach management headquarters under the supervision of the Communications Infrastructure Protection Committee to implement recovery measures and provide technical support.

The central administrative agencies responsible for the management of critical information infrastructures designate critical information infrastructures in their field of administration and implement protective measures. Protection guidelines are established by the central administrative agencies for critical information infrastructure managers to follow.

Critical information infrastructure managers hold the primary responsibility for protection and must assess vulnerabilities of facilities under their jurisdiction to implement protective measures. In the event of a breakdown of a critical information infrastructure due to disturbance or destruction, the relevant organizations must be notified and measures required for the recovery and protection of the communications infrastructure must be taken [3].

Organizations that support the protection of critical information infrastructures include the Ministry of Public Administration and Safety, National Intelligence Service, Ministry of National Defense, Public Prosecutor's Office, National Police Agency and Korea Internet Security Agency. These organizations also establish critical information infrastructure protective measures and provide technical support for prevention and management of security breaches.

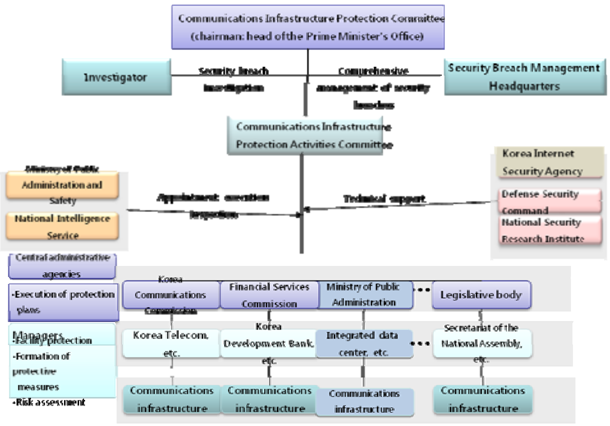
Communications Infrastructure Protection Committee
(chairman: head of the Prime Minister's Office)
Investigator
Security breach investigation
Comprehensive management of security breaches
Security Breach Management Headquarters
Communications Infrastructure Protection Activities Committee
Ministry of Public Administration and Safety
National Intelligence Service
Appointment execution inspection
Technical support
Korea Internet Security Agency
Defense Security Command
National Security Research Institute
Central administrative agencies
-Execution of protection plans
Korea Communications Commission
Financial Services Commission
Ministry of Public Administration
Legislative body
Managers
-Facility protection
-Formation of protective measures
-Risk assessment
Korea Telecom, etc.
Korea Development Bank, etc.
Integrated data center, etc.
Secretariat of the National Assembly, etc.
Communications infrastructure
Communications infrastructure
Communications infrastructure
Communications infrastructure

Figure 1. Critical Information Infrastructure Management System

III. Security Threats to Critical information infrastructures in the Administrative Sector

A. Attacks on Public Administrative Service Websites

Websites that service the public through critical information infrastructures of the administrative sector, such as the websites of local governments, are currently understood to be relatively safe from external infiltrations in their servers. However, there are hazardous elements found on other websites operated by local governments, which can jeopardize the security of such websites if such elements are analyzed and taken advantage of maliciously. In general, the vulnerabilities of websites with menus that contain sub-domains are cookie poisoning and cross website script vulnerabilities, which can be manipulated to gain access to some personal information of registered website users. File download vulnerabilities and factor modification can be incorporated into attacks to steal web application files and database access history and change posts made by other users.

Taking the online notice board for example, after session authentication, application factor modification can be used to read, modify or delete non-public posts made by other users; file download vulnerabilities can be taken advantage of to expose application source files; or insufficient script tag restriction settings can be taken advantage of to steal other users' session IDs to access their personal information. Because file extension verification for upload of image files on websites with inadequate security is insufficient, restricted extensions (ASPX, ASP) can be uploaded to generate certain files within the system. Such files then enable the upload of malicious programs, which are then used for remote execution of malicious commands to access databases, administrator accounts and personal information.

B. Attacks on Internal Administrative Networks

Development and management of critical information infrastructures of the administrative sector are frequently performed by a civilian business. In such a case, the critical information infrastructures may be insufficiently managed due to various reasons, such as the civilian business' heavy workload or budget shortage. This can result in vulnerabilities in servers, networks or PCs that can be taken advantage of by a third party to execute a malicious attack. Some common internal system vulnerabilities are as follows.

Server vulnerabilities can occur due to issues in account management, system/directory security settings, registry security settings and unnecessary services. Network vulnerabilities can occur due to issues in remote access control, log storage settings, anti-DDoS settings and unnecessary services. PCs can be vulnerable to unauthorized data access due to unnecessary services and non-use of a screen saver.

By taking advantage of such vulnerabilities, even closed networks with no external connection can be infiltrated using social engineering techniques and USB worms to steal information, which is then taken away from the premises on a USB or through a third party and disclosed on the internet, setting the network from which the information was stolen a target for attack.

Due to the nature of critical information infrastructures, system vulnerabilities must be removed by meticulously analyzing system stability and connection to other systems. Such security improvement may require substantial time and resources, so ongoing monitoring is required.

IV. Protection of Critical information infrastructure in the Administrative Sector

For improved IT security in the operational environments of e-governments and local governments, various protective measures, such as the application of information protection processes, facility security upgrade and server/network security upgrade, can be implemented to achieve a consolidated information protection and reliability of the communications infrastructures. In particular, information protection for critical information infrastructures in the administrative sector is divided into technical, physical and managerial aspects and executed accordingly.

TABLE I. Protection of Critical information infrastructure of the administrative sector

Security management		Details		
Technical	**Website**	Mock hacking	Performed on priority websites	
	Internal administrative network	Application system	Server network, etc.	o Security control settings, service access control, security system operation o Inspection of security policies, user authentication, etc.
		Security system	IDS, IPS Firewall, etc.	
		Personal user system	PC, etc.	
Physical	**Information protection assessment**	Physical aspect	Data room access control, power-supply control	o Physical access control, restricted area setting, installation of physical security facilities o Designation of a physical security facility manager, inspection of backup files o Power-supply control, etc.
Managerial				o Utilization of the KISA Infrastructure Information Protection Assessment Chart, KISA Infrastructure Protection Activities Inspection Chart and other methods o Information protection assessment based on local governments' activities and conditions

A. Technical Protection

Based on an analysis of various security breaches that can affect the stable operation of critical information infrastructures and the confidentiality, integrity and availability of information stored therein, technical vulnerabilities of the infrastructures must be identified to gain an understanding of the consequences of a security breach and form preventative measures. As such, the servers, network equipment, security systems and PCs that are part of critical information infrastructures must be analyzed and a security breach test performed to analyze the ensuing web service stability and possible scenarios of external attacks. [4]

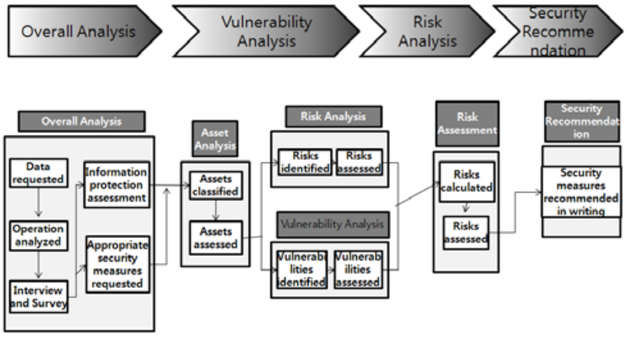

Figure 2. Vulnerability Assessment Methodology (KISA)

In order to remove the vulnerabilities identified through the analysis, short (6 months) and long-term (1 year) plans must immediately be established to continuously remove vulnerabilities. The technical measures to be taken to remove such vulnerabilities are as follows.

1) Prevention of security breaches and loss of key information through consolidation of server/network security settings

a) Consolidated account management, including consolidated authentication management and regular account policy reviews, for prevention of database access by unauthorized parties and loss of information

b) Consolidated access control, including consolidated remote access control and regular access control policy reviews, for prevention of access to key systems by unauthorized parties *c)* Consolidated operation management, including regular security patch application on servers/PCS and real-time anti-virus updates, for prevention of security breaches

2) Consolidated infrastructure security management, including the application of upgraded information protection solution, for prevention of exposure to potential threats

a) Implementation of integrated log management solutions that manage and monitor logs generated between different devices for systematic identification and analysis of threats

b) Implementation of anti-DDoS solutions and upgrade of existing information protection solutions for minimization of vulnerabilities in networking facilities used to service the public

B. *Managerial/Physical Protection*

Following a technical analysis of devices used in critical information infrastructures, the overall state of information protection by an infrastructure manager is analyzed to form customized information protection measures and plan their quantitative implementation. Information protection assessment methodologies established this way are presented to Korea Internet Security Agency annually. An information protection assessment assesses 12 areas of security control, which contain 89 sub-areas of security control. Each sub-area of security control is assessed according to the standards shown in Table II. The maturity of an area of security control is determined according to the outcome of an assessment of its sub-areas of security control.

TABLE II. VARIOUS LEVELS OF MATURITY OF INFORMATION PROTECTION ASSESSMENT

Level	Details of assessment
1	Sub-areas of security control are not being executed or are being executed without a set plan
2	An execution plan (procedures, schedules, budget) for some sub-areas of security control is set and documented
3	Sub-areas of security control are being executed according to a documented plan by the entire organization or have been executed
4	Assessment of sub-areas of security control continues to take place for a set period of time
5	Assessment of sub-areas of security control is completed and regular improvements are made according to the outcome of the assessment

Table III below shows the areas and sub-areas of security control assessed in an information protection assessment.

TABLE III. AREAS OF INFORMATION PROTECTION ASSESSMENT

Area	Sub-area
1. Information protection policies	1.1 Information protection policy organization
	1.2 Information protection plan
2. Risk assessment	2.1 Asset classification
	2.2 Asset allocation/management
	2.3 Security requirement review
	2.4 Risk assessment
	2.5 Vulnerability assessment
3.Structural management	3.1 Security structure modification control
4. Maintenance	4.1 Maintenance tools
	4.2 Remote maintenance
5. Media protection	5.1 Media display
	5.2 Media access management
	5.3 Media viewing/transportation methods
	5.4 Document management
	5.5 Media/record disposal
6. Security awareness/training	6.1 Security awareness/training
	6.2 Emergency training
7. Work continuity management	7.1 Work continuity management
	7.2 Information system backup/recovery
8. Physical/environmental protection	8.1 Physical access control/monitoring
	8.2 Electricity/communication cable protection
	8.3 Emergency electricity/lighting
	8.4 Environmental control
9. Personnel security	9.1 Personnel management
	9.2 Internal personnel management
	9.3 Third party security
10. Accident management	10.1 Accident management drill training
	10.2 Accident monitoring
	10.3 Security breach processing
11. Audit and attribution of responsibility	11.1 Auditable event generation
	11.2 Audit information management
	11.3 Audit monitoring/analysis/report
	11.4 Denial prevention
	11.5 Attribution of responsibility
12. System access control and communications protection	12.1 Account/password management
	12.2 Setting management
	12.3 Access control
	12.4 Failed access attempt management
	12.5 Notification of warnings during system operation
	12.6 Software faults/protection from malicious codes
	12.7 Service denial protection
	12.8 Confidentiality management

V. CONCLUSION

Korea is an advanced IT society and the majority of its key social infrastructures rely on communications infrastructures. Electronic invasions as well as natural disasters can result in the destruction and breakdown of such communications infrastructures, which can ultimately lead to the destruction or breakdown of social infrastructures that rely on the communications infrastructures.

The Korean government has established the Communications Infrastructure Protection Act which stipulates the designation of the communications infrastructures recognized as requiring protection from electronic invasions as critical information infrastructures. In the administrative sector, technical, managerial and physical measures must be taken to achieve ongoing security as attacks on websites of the administrative sector or internal administrative networks can stop the provision of administrative service to the public.

The number of designated critical information infrastructures is not high in comparison to the level of key social infrastructures' reliance on communications infrastructures. As such, an increase in designated communications infrastructures is in the best interest of the nation.

Therefore, critical information infrastructures must be continuously designated and accompanied by an efficient protection system in order to eliminate national and social vulnerabilities to acts of electronic invasion.

REFERENCES

[1] National Assembly: Critical Information Communication Infrastructure Protection Act (www.law.go.kr)

[2] Ministry of Public Administration & Safety, Korea Internet Security Agency: *Communications Infrastructure Protection Guide*.2009

[3] J. Chul-ki *"A Research on Cyber Security Threats to Critical information infrastructures and Their Countermeasures: With a Focus on the Broadcasting/Communications Sector."* vol. 9, pp. 34-36, August 2009

[4] L. Bodin, L. Gordon, and M. Loeb, "Information security and risk management,Communications of the ACM", vol. 51(4), pp. 64–68, 2008.

ISBN: 978-1-61208-105-2