Development of a Practical Guideline for IT Risk Assessment and Treatment

Background

As IT systems play core roles in various business activities in an enterprise, IT risk management that prevents and reduces damages by security incidents becomes indispensable for business continuity. IT risk assessment and treatment is a basis of effective IT risk management, and several international standards such as ISO/IEC 27005:2008 provide those guidelines. However, such guidelines are too abstract and need large quantities of cost and time to assess large-scale IT systems.

Objectives

The purpose of this study is to develop practical and convenient procedures of IT risk assessment and treatment for a large-scale IT system.

Principal Results

A practical guideline for IT risk assessment and treatment is developed based on a new IT risk assessment method, that divides a large-scale IT system into a number of security zones *1, assesses IT risk factors in each security zone, and integrates the assessment consequences into one of the whole IT system. This guideline defines logarithmic criteria (called levels) of (a) business impacts *2, (b) threats, (c) vulnerabilities, and (d) sources of threats, and provides templates of assessment consequences of standard assets. A list of countermeasures and those effects against incidents is also provided. The procedures of guideline are as follows:

(1) Identification of assets: dividing IT systems into security zones, identifying equipment units (hardware), information units (software and data), and perimeter units in each security zone,
(2) Evaluation of business impacts: evaluating three types of business impacts for each equipment unit based on asset values of information units on it (Fig.1 A [1]),
(3) Assessment of incident likelihood: identifying and evaluating levels of (a) threats and vulnerabilities on each equipment unit, (b) likelihood of bypassing perimeter units between security zones, and (c) likelihood of occurrences of sources of threats. Levels of incidents likelihood are estimated from (a), (b) and (c) (Fig.1 A [2]),
(4) Estimation of risk level: estimating risk level (a logarithm of expected damage by an incident) against a pair of threat and vulnerability for each equipment unit from results of (2) and (3) (Fig.1 A [3]),
(5) Risk treatment: identifying incidents over a given acceptable risk level (Fig.1 A [4]), constructing a set of countermeasures (Fig.1 B) in order to reduce risk levels (Fug.1 C), and selecting a set with a minimum cost if several sets are constructed.

A supporting tool that automates most of the above estimation and reference is developed, and can be used to decrease the cost and time for IT risk assessment and treatment process.

Future Developments

Feasibility tests will be performed, and the guideline will be improved with the test processes.

Main Researcher: Atsushi Futakata
Senior Research Scientist, Mathematical Informatics Sector, System Engineering Research Laboratory

Reference

T. Shimada, et al., 2009, “Development of an IT Risk Assessment Method for Large-Scale IT Systems”, CRIEPI Report R08020 (in Japanese)
A. Futakata, et al., 2008, “Development of Evaluation Method of Cost-Effectiveness for IT Risk Countermeasures (Part 1)”, CRIEPI Report R07024 (in Japanese)

＊1：Subnetworks, each of which has a proper security level, i.e. DMZ (Demilitarized Zone), an intranet server zone, and a core network zone.
＊2：Expected scale of damage to business activities by an incident.

A. an example of IT risk assessment (WWW server located on DMZ)

Security Zone	Equipment Unit	Levels of Business Impacts C	I	A	Threats Contents	Level	Vulnerabilities Contents	Level	Levels of Incident Likelihood	Risk Levels (C)	Risk Levels (I)	Risk Levels (A)	Risk Levels
DMZ	DMZ WWW server	3	3	3	**Theft of equipment**	5	**Lack of protection on device detachment**	4	1	9	9	9	9
					Destruction of equipment	5	**Lack of physical protection**	5	2	-	-	10	10
					Eavesdropping from linked external unit	4	**Lack of protection on illegal device connection**	4	0	8	-	-	8
					Illegal use of/t ampering with software from external device/media	3	Illegal boot from external device/media	3	-2	6	6	6	6
					Illegal use of/t ampering with software from external device/media	3	Illegal execution of software from external device/media	3	-2	6	6	6	6
					Eavesdropping on network	3	**Lack of physical protection**	5	0	8	-	-	8
					Tampering packets on network	1	Lack of physical protection	5	-2		6		6
					Illegal operation on console	3	Insufficient Certification on Console	3	-2	6	6	6	6
					Information disclosure from I/O device	3	Insufficient Certification on Console	3	-2	6	6	6	6
					Eavesdropping by illegal inline connection	3	Lack of protection on illegal device connection	4	-1	7	-	-	7

Consequences
Risk level of each incident on DMZ WWW server

[4] Risk levels over acceptable risk level (>7)

[1] evaluate business impacts on DMZ WWW server in view of Confidentiality (C), Integrity (I), and Availability (A).

[2] evaluate (a) in the text, and estimate (b) from (a) on perimeter units. With (a), (b) and (c), incident likelihood are estimated.

[3] estimate risk levels of C, I and A. The worst value of the risk levels becomes a risk level of incident.

* In each level, smaller value means smaller impact/likelihood.

IT risk countermeasures against the incidents with higher risk levels are selected.

B. an example of IT risk countermeasures

Security Zone	Equipment Unit	Countermeasures Contents	Effects
DMZ	DMZ WWW server	Locking of machine rooms and rack cabinets	prevent theft, destruction, connection of external device/media by protecting physical access
		Prohibition of all connection with external device/media	prevent eavesdropping, information disclosure and illegal installation of software
		Encryption of communication	prevent eavesdropping and tampering on network

C. an example of effects of the countermeasures (acceptable risk level: 7)

The risk levels are reduced by the counter-measures on equipment and perimeter units.

DMZ	DMZ WWW server	3	3	3	**Theft of equipment**	5	**Lack of protection on device**	4	-1	7	7	7	7
					Destruction of equipment	5	**Lack of physical protection**	5	-1	-	-	7	7
					Eavesdropping from linked external unit	4	**Lack of protection on illegal device connection**	2	-2	6	-	-	6
					Eavesdropping on network	3	**Lack of physical protection**	2	-3	5	-	-	5

Fig.1 An Example of IT Risk Assessment and Treatment