Introduction of Information Security Events and Processes

Student Name : Guo-zhan Huang Student No. : 92753019
speecher : professor Guo-long Gu

Abstract

In this writing we divide to three parts, information security events, Information security preventions and processes, Information assurance, to brief explain what the speecher said.

key word: VPN, identification

1. Introduction

Information security is more and more important due to the population of the Internet users or some systems are dependant on security heavily. We will found in the routine that much information couldn't be communicate each other due to the limits of authority are different. So we can know that security is important in some cases. In this speech writing we will focus on the prevention and the security events.

2. Information security events

In this section we describe elements in the information security that are information security events and it's expectation to begin this writing.

2.1 Definition of information security events

Information security event is combined three parts, confidential, integrity and availability by the professor Gu. The simplest way to explain protecting security is availability. The property of available is to make sure the privilege of accounts is mapping correctly to their owners, other owners couldn't be available if their have no complete permit by owners. The property of integrity is that keeping the data completely and the difference between availability and integrity is that weather the data had been moved from original place.

The last is confidentiality mean that different levels of privilege couldn't access between each other if the rules not permit. After all those three properties are to describe the information weather had completely in the physically and logically.

In the last we list some characteristics and classifies of the information security events that professor Gu had been talking in the speech.

Table 1. Classify of information security events

Infect with virus	Taroy programs in system
Eavesdrop signaling	Security spread by personnel
Destroyed in physically	Intruder from network

Table 2. Characteristics of information security events

Associating law has being developing.
Can easy to get intruding tools but hard to detect what is intruder Tradeoff of comfortable and security.
Across several areas, countries.

Now we can know what the information security events are but we don't know when the events happen and We will talk below the subsection.

2.2 Expectation of the information security events

The professor Gu say the expectation of the events in the speech. We list below.

$$\text{(The expectation of information security)} = \text{(Weaknesses and Intruding positions X Intruding events)* (probability of intruding events)} \tag{1}$$

Weaknesses and intruding events are meaning what's the leaks in our system and the opposite of intruders. Now we can know what are the events that would be happened but we also have to find the opposite probability. So we can know the expectation and used it in indicate intruding probability of the system in simplest way. We know what the events are in the system and next we will talk about common prevention of intruding.

3. Information security preventions and processes

Before discuss about prevention we have to understanding what the steps of intruding are. Behind comprehend the steps we can know how to prevent the intruders and the professor Gu said some concepts of prevention.

3.1 Steps of intruding

We know the event by foregoing and now have to understanding the relation between the intruding events and the leaks that are methods to hack. The professor Gu had divided several steps to describe those methods step by step from outside to inside. We list below:

Table 3. Stages of intruding

Stages	Brief explain
Reconnaissance	Using public information to gain the necessary information of intruding.
Probe, scanning	Sending specific packet to the host and gaining useful information.
Exploit	Intruding system.
Keeping access	Friendly to access system.
Covering the track	Let system or personnel didn't know the system is attack

We can find that the intruders are outside the organization in this list but the intruders are normally inside the organization in reality.

3.2 Prevention

The professor Gu had said some concept that had divided several layers that are the value of the levels. The most important thing is keep in the center of circle, the less important is put in the outside. Before this concept the professor had said that the events were ordered by the happened time of events and we can clearly understand how to process those events when the intruders are ready in the system.

Table 4. Stages of prevention

Stages	Brief explain
Before event	Prevention, management, backup
In the event	Monitor, detect, obstruct intruders
After event	Recovery and quickly response
Event terminated	Analysis, identify resource of attack

3.3 Safe requirements in the Internet

The requirements in the safe in the Internet are more important when the users grow. The professor Gu had divide 3 parts to easy understand the flow of prevent safe. We pain in below.

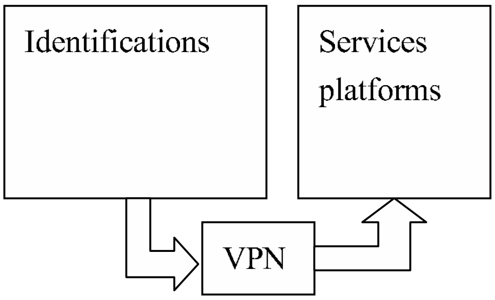

Figure 1. Safty flow of Internet

The identification is to distinguish what personnel are belonged to our group. It is functioned to filter the out-group personnel and sent permit message to VPN. The message in the VPN [1] , virtual private network, is provided to send message in private tunnels. When these message are sent into destination will be filter again in their platform by firewall or intruder detect system. And last problem is to manage all system architectures. The professor also said that VPN had popular in this time due to it could bring private tunnels for each organization. But the serious problems always produces by internal personnel.

4. Information assurance

Productions of security are offered a belief that reduced degree of harm but not focus on utilization of system. So productions of security are reduced the risk events not uncertain event, we also know these events in risk by reading aforementioned paragraph. So assurance in the information security is based on risk not utilization.

5. Conclusion

The professor Gu quoted that Security is a process not a product to conclude all. The security issues are a tradeoff between utilization of system and probability of risk. The basic remedy is to keep the human morality high.

6. Reference

¡1¿ R. Shirey, *"RFC 2828 Internet Security Glossary"*, pp. 189, May, 2000