An Research about ISPs' role as Managed Security Service Providers

Yang-seo Choi*, Dong-il Seo*
* ETRI Network Security Architecture Research Team
{yschoi92, bluesea}@etri.re.kr

Abstract — **Internet attack incidents have steadily increased along with the increase in Internet users. To protect systems and networks from these attacks, advanced security systems have been developed. Now that these security systems are operating, their successful management is more important than the purchase and establishment of new information security systems. The acquisition of good systems is ineffective and financially wasteful unless they are managed properly. Adequate management policy has recently become the focus of users. In other words, for companies and educational institutions with their domains, capital expenses are enormous to bear, and good security staffs are difficult to find, for which reasons outsourcing vendors or Managed Security Service Providers (MSSPs) that manage and operate the information security systems of certain domains become very appealing. Today, customers expect ISPs to perform MSSP services that used to be carried out by the security companies. This document presents the role and necessity of ISPs as MSSPs.**

Keywords — **MSS, MSSP, Security, Hacking, Management**

1. Introduction

In year 2000, the powerful DDoS attack occurred and caused tremendous damage, which awoke people to the importance of information security. The surge in the number of Internet users resulted in the provision of various services via the Internet. However, due to the lack of resources directed toward managing network security, the damage was inevitably overwhelming. After all, security systems have been developed that shield information security systems and networks from the constantly increasing and varied attack incidents; however, for information security, an effective management system is far more important than the purchase and establishment of new information security systems. That is, regardless of how effective the systems are, they will be a waste of money unless they are managed well and their functions used properly. Hence, managing security service is being held in high repute. However, the specific networks-managing companies or schools can't afford not only to dedicate staffs to security but also huge costs, for which reasons the outsourcing has been increasing to manage and operate information security system of the domain. The MSSP (Managed Security Service Provider)[1] that used to performed by the established security companies is recently much expected to be carried out by ISPs(Internet Service Providers). Accordingly, this document speculates on the role and necessity of ISPs as MSSPs.

This document consists of the following: Chapter 2 identifies MSS that the established MSSPs provide, and defines MSS. Chapter 3 analyzes the role of ISPs as MSSPs defined in this document. Chapter 4 presents the conclusion.

2. Security Service Provider

2.1 MSS & MSSP

MSS represents Managed Security Service. MSS generally includes remote and local security control for infrastructure such as networks, servers and databases, analysis of security attack events, management support for security equipment, and security consulting and maintenance.

Companies that provide these MSS are called Managed Security Service Providers (MSSP).

It was in year 2000 that the concept of Managed Security Service first emerged. During the first quarter of that year, the leading MSSP companies like Counterpane, Riptech, OneSecure, and Guardent appeared. In Korea, the MSSP companies including NetSecure Technology, Cyber Patrol, Coconut, and HackersLap announced their identities as MSSPs and started providing security services [3].

2.2 Security Services Provided

In addition to the security services previously mentioned, the following services are now being provided. It is thought that these multiple services are being added and modified in response to the recent circumstances of the Internet and changes in hacking techniques.

- Managed Firewall
- Managed VPN
- Managed IDS
- Managed AntiVirus
- Managed Filtering (of web content)
- Managed Scanning (analysis of vulnerability)

The definition of each service is self-explanatory. Managed Firewall means management of existing firewalls, Managed VPN means providing a VPN function. The majority of managed services utilize outsourcing to provide administration and management. Managed Filtering signifies the blocking of packets based on web content. The types of managed services provided by US companies are shown in Figure 1 [4].

As discussed above, the recent addition of supplemental security services has added significantly to the benefits of

Table 1. Managed Security Services by MSSP [4]

Provider	Managed Firewall	Managed VPN	Managed IDS	Managed AntiVirus	Managed Filtering	Managed Scanning
Allegiance Telecom	o	o				o
AT&T	o	o	o		o	o
Aventail Corporation		o				
Bangalore Labs	o	o	o			o
Cable & Wireless	o	o	o	o		o
ClearPath Networks	o	o	o	o	o	
Guardent	o	o	o	o	o	o
Interliant Inc.	o	o	o	o		
Internet Security Systems	o	o	o	o		o
Network Associates Inc.	o			o		o
SecureWorks	o	o	o			o
TruSecure Corporation	o		o	o	o	o
Unisys Corporation	o	o	o		o	o
VeriSign Inc.	o	o	o			o

network security. The original administrative services for security equipment were highlighted by managerial aspects such as the operation of security equipment, consulting, and maintenance. Today, actual services for networking information security are being provided. As MSSs have evolved in accordance with these changes, ISPs (or NSP) with network infrastructure have been spotlighting as new MSSPs.

3. ISP as MSSP

3.1 Position of ISPs as MSSPs

As stated in Chapter 2, since 2003, ISP companies debuted as MSSPs. According to Gatner's 2003 reporting data, the preference for MSSPs changed from the existing security company providers to ISPs (NSP)[5].

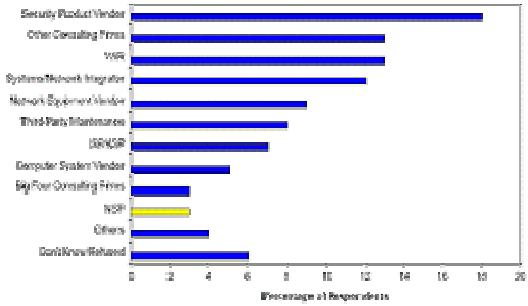


Figure 1. 2001 MSSP Preference [5]

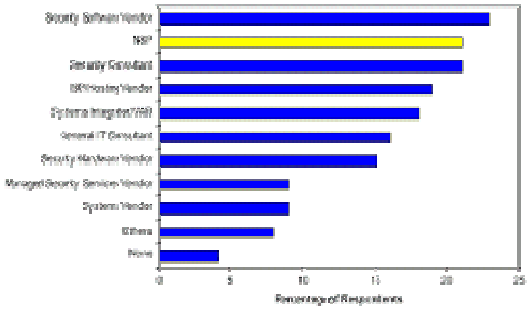


Figure 2. 2003 MSSP Preference [5]

As security services provided by MSSPs became a form of actual security service for network security from a managerial perspective, the expectation that ISPs should perform the role of MSSPs gained acceptance.

3.2 Role of ISPs as MSSPs

What reason is there to expect that ISPs should perform the roles of MSSPs? It is because ISPs have networking infrastructure. Ultimately, the development of network security alleviates concerns about attacks and threats through the systematic integration of all networks beyond the previous elementary level of system protection. For this eventual development, information security products and technologies such as F/W, IPS, Application Gateway and system security will be integrated systematically. In particular, IPS will play a far more significant role because it is more advanced than the current Signature-based attack detection and will be able to identify traffic trends in real time, and detect and block attack packets in accordance with the transitional changes.

At this point, the most important aspect is how promptly and precisely sources of intrusion can be detected. To achieve this aim, it is critical to be able to discern in real time the networks' traffic patterns in addition to outlying information. Consequently, the ISPs that can process this kind of information in the simplest and fastest way are second to none as MSSPs to protect networks in the most precise and swiftest manner.

Beyond the boundary of simple managed services and general information security services, ISPs should develop and apply information security technologies for global networking security based on firm investment. This does not mean mere financial investment, but also the solidification of the security of related ISPs and the provision of adequate security services, resulting in added value. Due to the advantages that ISPs have, it is forecasted that ISPs will occupy a dominant position over MSSP companies.

3.3 Identity of ISPs as MSSPs

Until now, an emblematic ISP company that performs the roles of MSSP is AT&T in the United States. AT&T provides Managed IDS, Managed Firewall, Managed VPN, Managed Filtering, and Managed Scanning for Managed Security Services as shown in Table 1 [4].

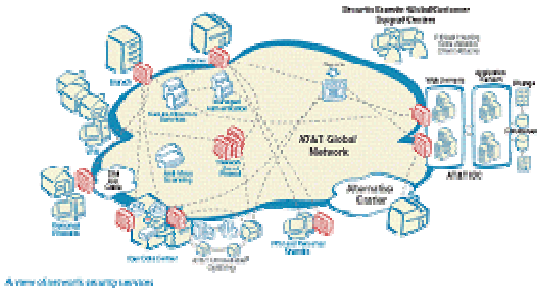


Figure 3. Network Security Service of AT&T [6]

Figure 3 displays the conspicuous advantages of ISPs as MSSPs, as emphasized in this document. That is, ISPs are able to discern attack situations at multiple positions on global networks and promptly detect intrusion and establish barriers to future attacks.

3.4. Managed Security Services of Korean ISPs

Until recently, Korean ISPs were unable to maximize their advantages as ISPs in providing managed security services. They were merely performing the same services, and only those services, that conventional security companies could perform. The exception was Dacom, which in September 2004, obtained a patent called "Network-based Integrated Security Management Service Networks,"[7] a business model capable of controlling and governing, from a centralized position, the detection and response solutions against a global network of worms, viruses, and hacking, based on a nationwide level of integrated security censors. This service that Dacom launched after patent acquirement is the integrated model for providing security services that capitalize on the previously addressed advantages of ISPs.

4. Conclustion

In summary, the key points of this analysis are that as the Internet developed, a host of security equipment was used for the prevention of varied types of attack incidents. However, the management and operation of such security equipment was difficult. Consequently, outsourced services performing this management capacity were developed, but only managerial security services like equipment management, analysis of security attack incidents, and security consulting were provided.

Recently, with the recognition of the importance of network security, the actual security functions used by network security technologies have been adopted and provided by security services. These security services include the following:

- Managed Firewall
- Managed IDS
- Managed VPN
- Managed Filtering
- Managed Scanning

The most effective way to provide these services is to collect attack information on global networks, analyze it in real time, and block the attacks. ISPs are best equipped to perform these types of detection and blocking of attacks. They can discern in real time attacks occurring on networks managed by corresponding companies because they are equipped with nationwide network infrastructure. Because of this advantage, ISPs have become more popular than security companies as MSSPs.

AT&T started as the leader in providing security services, taking advantage of its ISP function. In Korea, Dacom achieved a patent related to these services. In the future, ISPs will create added value by developing and providing comprehensive security services, while complementary security technologies will be constantly developed.

REFERENCES

[1] Lisa Phifer, "Managed Security Service Provider," ISP-Planet Survey, ISP Technology, 2001

[2] Lisa Phifer, "Managed Security Service Provider," ISP-Planet Survey, ISP Technology, 2003

[3] Hwang Tea-sun, "International and national managed security services market, and technological trends," NetSecure Technology's Column, Computer World, 2003

[4] ISP-Planet, "Managed Security Service Provider, Participating Providers Chart," ISP-Planet Survey, ISP Technology, 2003

[5] Elroy Jopling, "NSPs in Managed Security: What a Difference a Year Makes," AV-20-6654, Gatner, 2003

[6] AT&T, "AT&T OverView Security Services", AT&T Security Services Documents, 2004

[7] Dacom Corp., "Network-based Integrated Security Management Service Networks," Korean Intellectual Property Office 10-2003-0098647, 2004

[8] Kathleen M. Adams, "AT&T Internet and Network Services," DPRO-90894, Gatner, 2004

[9] Matthew Kovar, "Special Report: Next-Generation Network Security Requires an Adaptive Approach," Yankee Group, 2004