Incident Response and the Role of External Services

Andrea Rigoni

Business Development Manager - Government Sector
Symantec Corp.
Andrea_Rigoni@symantec.com

Abstract: Managing security is a complex task combining many aspects and services. While some of the services usually are operated internally to the hosting organisation there are others that can be outsourced to security professionals and firms specialising in IT-security services. This document provides an overview on such services and discusses their options for operation.

1 Introduction

The effectiveness of any countermeasure has always been considered limited in time, either because of problems arising within protection mechanisms, or the discovery of new vulnerabilities and threats; however, such a concept has only recently become part of security definitions and objectives. Any countermeasure system must therefore be supported by awareness capacity in terms of new vulnerabilities and threats. Furthermore, if incidents were unfortunately to occur notwithstanding the existence of an effective protection infrastructure, quick identification and correct management are crucial.

The two aspects mentioned above are often known as Real Time Security Monitoring and Incident Handling. In such a context, monitoring means incident identification, which is not to be mistaken with the monitoring of systems and networks to control correct operativeness.

Indications of such an approach can be found in many national and international security documents of the past years, though it is only lately, with the increase in the number of attacks and security incidents, that the indispensable nature of such functions has been acknowledged.

The concepts of incident management and security control and monitoring already appeared in the BS7799 Part 1, but has been further developed in the ISO17799 where it got the required importance.

A lot of international standards are addressing today Incident Management and Incident Response. Furthermore, ENISA is promoting the adoption of National CERTs with the purpose to facilitate the cooperation among the CERTs of private companies and public administrations.

As for international indications, The Information Security Forum adopted the previously-described approach, supported by a risk management methodology, known as FIRM, that since the first pages defines security as a set of three areas: incident prevention, incident detection and response. Today real-time security monitoring cannot be achieved by simply purchasing technological devices, though the market does offer a wide range of products to this end. The capability to correctly launch some key processes of the security cycle is also necessary. The components that determine the quality and effectiveness of such processes are the following:

- *Time coverage*: new threats spread within a few minutes, whatever the time and geographical area. Monitoring must be ensured 24 hours a day, 365 days a year, continuously and in real time. Indicatively, 6 to 10 people are necessary to cover 24 hours.

- *Knowledge*: the analysis of security events requires a very high level of competence that must be maintained in time. The analysis of new threats, as well as the choice of adequate procedures to manage the incident, requires very specific knowledge of the technologies used in the organisation, as well as consolidated experience in security analysis.

- *Knowledge base*: access to a security knowledge base is fundamental to enable incident analysis activity and to determine incident management procedures.

- *Identification and response to incidents*: since people manage identification and response activities, it is crucial to have the support of correct management processes and technological platforms. It is advisable that processes pertaining to the identification and response to incidents be compliant with acknowledged internal standards such as BS 7799.

- *Technology*: several hardware/software platforms support the functions of monitoring and response to incidents:
    - Log centralisation systems
    - Incident tracking systems
    - Trouble ticketing systems
    - Systems for the realisation of security portals
    - Centralised systems for security control and management.

The market offers several services to support the knowledge of new threats and vulnerabilities, as well as the launching and management of identification and response processes to the incidents describes below.

2 Managed Security Services

Managed Security Services (or MSS) include two categories of very different services:

1. Security Management
2. Real Time Security Monitoring

2.1 Security Management

The management services offered by a Managed Security Service Provider (MSSP) have the purpose of supplying ordinary and extraordinary management of security devices, in the form of outsource services. In particular, the security deivces are managed according to the three following aspects:

- Fault management
- Configuration management
- Performance management

Fault management manages client security devices to make sure they always operate properly. This is usually, though not always, achieved through an extended service on the 24h.

Some of the typical fault management services include:

- The periodic check-up of security devices to identify possible problems
- The notification to customers every time that, for any reason, the security devices ceases to function, and assistance/guidelines concerning appropriate measures to solve the problem
- Periodic reports to customers that summarizes the operational situation of their security devices over a pre-determined period of time.

Configuration management is used by the customer to outsource to the MSSP the configuration of his/her security devices. The expert responsible for configuration management usually deals with the following aspects:

- Modification and upgrading of the applications supporting security devices, and of the operative systems
- Modification of the policies and signatures applied to the security devices
- Daily, weekly or monthly reports listing all the new upgrades and modifications to the clients' security devices.

Performance management involves the collection and presentation of statistics on the performance recorded on the clients' security devices. The reports include the following:

- Statistics on the speed and efficiency of the client network
- Identification of internal bottlenecks penalising network performance
- Reports on overall performance, consolidating all the log data generated by the clients' security devices.

2.2 Real Time Security Monitoring

Security monitoring requires a high degree of competence in the security environment, as well as sophisticated architecture to support data analysis on different devices through a global organisation.In the context of the monitoring services offered by the MSSP, the word outsourcing must be taken cautiously: services offered from the outside do not replace internal control, and the security control room remains within the organisation. External services are to be considered as a useful support in identifying incidents.

Real Time Security Monitoring services are made up of the following functions:

- Data collection and standardization
- Data mining
- Automatic correlation of security-related events
- Response to events
- Event report

Data collection and standardization is a process in which data related to security devices (firewall log, IDS alert, etc.) are collected and transformed into a standard format, despite of the device nature and provider. Data standardisation is essential for efficient security monitoring, since this enables the MSSP to use a set of standard queries to analyse the security device data and to isolate traces of dangerous activity.

The data mining process is made up of an automated system that constantly queries security devices to identify any sign of dangerous activity, thus separating suspicious from legitimate network traffic.

It is probably the central technological element in monitoring processes:

a client has to make sure that an MSSP is able to scale down its capacity in terms of data mining as the devices connected to the backend architecture increase. In other words, the MSSP must be capable of developing ever-more sophisticated queries as new devices are added to the network. Nevertheless, increasing the number of queries does not necessarily mean improving the data mining process. In this sector, the quality and constant fine-tuning of queries are extremely important, as well as the timely creation of new queries able to constantly reveal evolving harmful activity. It is only thanks to highly sophisticated data mining that an MSSP can ensure efficient correlations between data and attacks.

Another essential component for a truly effective monitoring service is the automated correlation of security-related events, in other words, the automatic grouping of specific harmful activity traces, using logical criteria such as source, nature and destination of the attack. Thanks to this process, attacks are rapidly reconstructed, and analysts can view the entire attack. Without automatic correlation, security analysts would be obliged to reconstruct the attack sequences by manually going through millions of lines of data recorded by the security appliances. Needless to say that such an operation is too expensive in terms of the time involved and too complex at any scalability level, even on networks with low traffic volumes.

The response to events that have repercussions on security follows and depends on the security analyst's examination of the data generated by the correlation process. According to the nature of the event, the range of actions can vary from simple client notification to immediate communication of the event to the competent police authorities. The availability of a service enabling the analysis ofsecurity events by experts over the entire time arch (24x7) is decisive for the management of any security service. Event reporting is the process adopted to notify clients about events identified on their network that have an impact on security. According to the nature of the event, the reports can be transmitted immediately by voice, e-mail, or by real-time notifications published on the Web portal, or even, by means of periodic reports.

Monitoring services are usually offered for security platforms that supply significant information on events (firewall, host and network intrusion detection system, etc.). To enable effective real time security monitoring, a MSSP must have all the above-mentioned features. Protection against vulnerabilities, real-time risk identification and management for network security are impossible to achieve in the absence of just one of these services. The difference between security management and simple monitoring lies both in the availability of top level professional knowhow and a complex technical architecture able to perform global data analysis on several platforms. This aspect was stressed in the article 'Top Guns' published in the Information Security review: Security software has made great progress in the capacity to consolidate, correlate and analyse events and data logs on several appliances such as firewalls, IDS and routers. However, according to experts at the control stations of the SOC (Security Options Centre) of MSSPs, when analysing events with security impacts, the most reliable, though oldest, tool is intuition.

3 Early Warning

The most numerous and frequent security incidents having affected organisations worldwide derive from external threats such as viruses, worms and other forms of malicious codes. Such threats are global, since they indiscriminately affect organisations anywhere in the world, and have not been devised to attack one specific organisation, even though they have lately become a means for perpetrating targeted attacks by exploiting the technical vulnerabilities and weakened defence of organisations during emergencies. In all recent famous cases (Blaster, MyDoom, Sasser, etc.), only a few hours passed between the first attack and the moment of maximum diffusion.

This data, together with the fact that no environment is nowadays completely protected against any vulnerability, stresses the importance of adopting preventive and proactive strategies. So-called early warning services, or preventive notification, help organisations learn in advance about emerging vulnerabilities and threats, and adopt correct countermeasures to prevent the phenomenon before it affects the organisation.

Early warning services can be divided into the following two categories.

3.1 Vulnerability Notification

This is the service that warns an organisation any time a new vulnerability is revealed. However, since a consistent number of vulnerabilities are discovered every day, the most advanced services make it possible to receive notification only for vulnerabilities concerning the technology and products installed in the organisation. Free services also exist, in the form of mailing lists; nevertheless, they do not guarantee timely notifications, nor do they allow any choice as to the kind of notification one wishes to receive.

3.2 Threat notification

*V*ulnerability in itself is insufficient to represent a risk for an organisation. It is the existence of technologies and methods that exploit vulnerabilities that make them possible vectors for attacks and violations. Threat notification services are able to rapidly identify the existence of activities that could exploit vulnerability and to send a notification to member organisations. There are currently not many threat notification services, since they require a large, real-time analysis and intelligence network of the provider, able to immediately reveal the early signs of vulnerability exploitation. Together with the notification of new threats, early warning service providers supply a detailed description of the phenomenon, a list of vulnerable systems, possible impacts, propagation methods and actions suggested for risk mitigation or cancellation.

4 Incident Handling

Not all security infrastructures, even the best, are able to supply absolute protection guarantees for the IT system. Notwithstanding the huge progress achieved in the past years by security enhancing devices, their effectiveness is still limited, and in no case absolute. Adequate structures to manage all the events (incidents, frauds, attacks, malfunctioning, etc) that threaten service and = information continuity are therefore necessary.

This organisational structure is usually known as CERT (Computer Emergency Response Team), and is responsible for receiving, analysing and managing incidents pertaining to information security. Furthermore, it also has the task of coordinating and monitoring several activities that are fundamental for ensuring an organisation with the most adequate security levels.

In the presence of a CERT, an organisation will be able to manage all incidents centrally. The activation of a CERT will namely enable an organisation to:

- Optimise resources, time, costs and incident management tools thanks to the centralisation and coordination of activities
- Safeguard its information heritage, preserving privacy, integrity and availability, even in compliance with the privacy protection measures
- Limit the incident occurrence and probability through monitoring and prevention activity
- Constantly monitor the security status of its information system.

Since the activation of a CERT is very complex and time-consuming activity, it is advisable to resort to a specialised company that can offer advice as to the following:

- Definition of an organisational model
- Definition of the technological architecture of the security operations centre that will host the CERT
- Launch the CERT, define processes and procedures
- Specialised resources for personnel training and incident management
- Support services (real-time security monitoring, early warning).

5 Specialised Help Desk

Specialised help desk services are very useful; whenever needed, they supply necessary support and expertise for problem/incident solving. The range of specialised help desk and support services is vast. Often, it is the security technology producers themselves that supply support services, though they are in most cases limited to their own platforms.

Below is a list of some factors to consider upon the purchase of a help desk service:

- Hours covered (working hours or 24h)
- Typology of support (basic or specialised)
- Required expertise
- Presence of personnel specialised in the products used by the organisation
- Ticket management modality in relation to the level of seriousness of the call
- Security procedures
- Service levels
- Existence of a portal (informative or interactive).

References

[BS7799] Information technology. Code of practice for information security management, British Standards Institute (BSI), 1995

[ISO17799] Information Technology - Code of practice for information security management, International Standards Organisation (ISO), 2000, 2005

[ISO 27001] Information technology -- Security techniques -- Information security management systems – Requirements, International Standards Organisation (ISO), 2005