I met Chuck Adams, general manager of the ProWatch Secure® Security Services Group at NetSolve, Inc. (<http://www.netsolve.com>) at the Network World Security Events in the summer of 2001. Several months ago, he sent me the following thought-provoking essay about managed security services. In this column, we’re publishing an edited version of his comments with the kind permission of Mr Adams. In the following text, 'I' refers to Chuck Adams.

***

I would like to clear up confusion in the managed security services market and provide an explanation of what services customers should be asking managed security providers for in order to ensure they are not making themselves more vulnerable to compromise. Over the last 15 years, I have had the unique opportunity to witness the evolution of the information security industry from a non-existent, military-only issue to the full-scale selling of fear, uncertainty and doubt that exists today. My perspective is unique in that my exposure to security begin in the trenches of operations service delivery and has developed over the years to the consultative and strategic levels.

It is fundamentally important to remember that the entire security industry exists because of fear. This motivation may be fear for our safety or fear of losing information that is valuable and whose absence or corruption can cripple business. It is this fear that is fueling the desire for solutions. Solutions that reduce fear, either services or technologies, are becoming very complex, expensive, and difficult to understand. This increasing complexity is leaving our business and home networking environments more vulnerable and setting the stage for a solution to managing security other than depending solely on vendor offerings.

Managed Security Services (MSS) consist of the following four basic categories:

(1) Proactive professional services that offer expertise to an end-customer to answer the key questions about an enterprise's security. These services typically approach risk assessment and management through services like network vulnerability assessments, electronic mapping exercises, network architectural and design reviews, policy development, and technology or policy implementation / integration services.

(2) Managed infrastructure services provide ongoing monitoring and management services for systems and networks. These services cover network servers, routers, switches, firewalls, and intrusion detection sensors. The three main service components necessary for effective management of infrastructure devices of these types are

* fault monitoring and management,
* configuration management, and
* performance monitoring and management.

Unfortunately, some managed security services companies monitor only the firewall and intrusion sensors without considering the other infrastructure devices. This narrow focus is a
recipe for disaster because security involves the entire network. One must be confident that all of one's security technologies and primary protection tools are accurately detecting and reporting real and potential security incidents as they occur.

(3) Security monitoring services collect data from security and network sensors, correlate of these data, detect security events, and analyze and report on these events as they are detected. These services are predicated on the principle that monitoring alone is inadequate: in addition, one must provide proactive notification of vulnerabilities as well as analysis and resolution of errors and events involving security devices. All these functions are necessary elements of effective security management. Thoroughgoing security management requires

* tools to detect violation of policy and report the event fast,
* preparations in place to monitor and provide expertise for event analysis,
* the ability to compare the potential effects of each incident based on accumulated and systematized knowledge of exposures, and
* response to the event in near-real-time on behalf of the customer.

There are a few providers that successfully combine security monitoring and managed infrastructure services; this combination results in an effective security management solution that helps reduce fear. This full monitoring and management solution acts as a single provider to detect, analyze, and respond to an incident on behalf of the customer and to mitigate the effects of an event.

(4) Reactive professional services include incident response, evidentiary collection, and litigation support. These services can be delivered by highly specialized professional services firms. As more security technologies are deployed and more intrusion attempts are detected, reported and managed, these reactive services will become more defined and will be delivered by a broader range of service providers.

In summary, effective security management, whether provided in-house or by an external service, must be a function of network management and that viewed as an independent, isolated operation. Since data and information security requirements are distributed throughout the network, so must the processes, policies and services used to enhance the level of protection of this information.

***

For further reading:


***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.
