Developing a plan for network security

Contributed by David Noel-Davies

Security is an ever moving target that must be continually managed and refined to ensure appropriate confidentiality, integrity, and availability of the services and systems that are critical to your business, as well as the valuable information that is often at the heart of the organisations we defend.

The stream of news stories highlighting loss of customer information and proprietary data (among other drivers) are prompting many of us to take a step back and re-evaluate the infrastructure at large, and our security tools within that infrastructure.

In your case, you're wondering how network tools can help in creating up-to-date security policies.

A flippant, and I suspect prevalent, answer to that question would be that tools aren't for developing policy, they're for helping to enforce your policy. Such a view falls short in my opinion, because while policy enforcement may be a tool's greatest contribution to your security programme, our tools often log activity that we can channel into a feedback loop that informs changes to policy. In other words, knowing what the tools are uncovering positions us to use this information to evolve (or update, if you prefer) our security policies.

There are well known, bread and butter tools that often aren't though of as policy tools. However, many of them can have a role in shaping your policy if you use them that way.

Vulnerability scanners - these scanners can help you determine patching policy. Once you know what vulnerabilities are exposed, you can make decisions about what can and can't be tolerated in the environment, time-frames and patching SLAs, and firewall rules.

Application security scanners - can inform your decisions about secure coding standards, and whether you make any investment in code scanning technology to help automate both implementation and enforcement of any standards you put in place.

Flow data and Network-based Anomaly detection - knowing your typical network behaviour can highlight common activity that you might want to curb via policy or other tools. Both these technologies provide visibility into your network traffic.

IDS - a well-tuned IDS can provide information about attacks coming into your environment. This information can inform decisions of which technologies you deploy architecturally. You might notice attacks against one operating system in particular, and require a new deployment to use a different operating system as part of your defence strategy, or perhaps you uncover worm activity trying to spread from one network to another, and use this to create a policy that segments both network in part or in full.

The above aren't the only well established technologies in the security realm, and of course the list of examples could go on. Emerging tools too

In addition to the established tools, new tools are always being created. Some succeed and some don't, and many, though in early stages of development, are worth considering.

Some strong examples that come to mind with regard to tools that can live on the network are network risk mapping applications, and data loss prevention.

Network risk mapping products sift through vulnerability data and network device configurations and help you prioritise which issues to resolve first. Data can be based on criticality of nodes that you define, directly vulnerable hosts, non-secure configuration of network equipment, and hosts most susceptible to compromise when leapfrog attacks are factored in.

Data loss prevention tools (often referred to as DLP) can shed more light on what people are doing, how you need to educate them, and what your common business risks are. DLP products comprise a broad solution category and provide security for information or concepts. Facets of the idea are implemented in three distinct ways, usually breaking down along the lines of data in motion, data at rest, and data in use.

DLP for data in motion is implemented using sensors at the outermost point of the network perimeter and/or at network aggregation points. Sensors examine information in transit to see if the traffic triggers any rules designed to prevent proliferation or compromise of sensitive data. For instance, a rule may be in place to log any attempts to send intellectual property to a destination outside of the network. Similarly, rules can be created that log when personally identifiable information, customer lists, or pricing information is sent out. These sensors can generally integrate with other security systems such as proxies or mail transfer agents to block the transmission of such data.

DLP for data at rest is implemented using network-attached devices that scan nodes on the network to detect the proliferation of sensitive data or data that otherwise violates a rule, such as those used with data-in-motion sensor systems. These network-attached devices are also generally able to provide the administrator a means of 'registering' or 'fingerprinting' sensitive documents, importing sensitive data, and monitoring end nodes for the existence of these documents. Data-at-rest DLP systems are also able to send fingerprint information, or 'document signatures,' to adjacent DLP systems (such as those for data in motion) to strengthen the controls that detect or prevent information leaving your network.

DLP for data in use is implemented using software agents deployed on the user desktop that are complementary to other desktop security capabilities such as software firewalls, HIDS/HIPS, and antivirus. These agents let the administrator ensure that sensitive data does not leave the company through an unapproved I/O channel, such as an un-encrypted USB drive, or through a user's Webmail account.

The concept of DLP encompasses an evolving set of technologies that work together to provide security of information.