NETWORKWORLD

This story appeared on Network World at
http:// www.networkworld.com/columnists/2008/013008-jericho-network-security.html

The future of network security

Plus: 10 questions to ask when determining your future security architecture
The Jericho Forum Outlook By David Lacey , Network World , 01/31/2008

Enterprise connectivity is exploding, driven by globalization, convergence, virtualization and social computing. As corporate perimeters dissolve, the security focus switches towards application and data-level security solutions. The question to ask is what are the longer-term implications for network security? Will it become redundant or could it grow more powerful? Only one thing seems certain: It will be different from today.

Who needs network security? Why don't we just build encryption and antimalware protection into end-points and simply enjoy open networks? From a security perspective that's always best and it's in line with the Jericho Forum vision. But in the real world it's not so simple. At the very least we need protective measures in networks to guarantee availability and performance. Beyond that there is huge potential to deliver value through security features in networks.

In fact there has always been more to network security than users realize. Fallback, monitoring and filtering are ever-present but invisible to endpoints. Many application owners believe their systems operate on top of a pure IP infrastructure, but nothing could be further from the truth -- enterprise networks are heavily structured.

Today's network products boast an impressive and growing array of single-point security solutions, ranging from simple authentication mechanisms to full-blown identity management. (Learn more about identity management products in our Identity Management Buyers Guide)

Related Content

Taking advantage of network-based security features is difficult in that geography and topology are major factors. They dictate ownership boundaries and legal jurisdictions and it's hard to establish a set of choke points from which all network traffic can be monitored or controlled.

Management domains don't map neatly onto the precise scope of application systems and legacy

equipment presents local incompatibilities. Nevertheless, gateway devices are a convenient point for securing central databases. And complete network coverage is not always essential for value to be derived from security analysis because useful intelligence can be derived from samples of traffic.

There are also distinct advantages in locating security measures inside networks. You gain a richer picture of user behavior, enabling individual user activities to be assessed in the context of a broader community. In fact, visibility of events and understanding of context are the keys to effective security and risk management.

The significance and legality of user actions is dependent on context, varying according to user authorization level, sensitivity of data, location of source, method used, and time of day. As one of the 11 Jericho Forum principles states: "Assume context at your peril."

One of the biggest security concerns today is the insider threat. In response to this, you can deploy many interesting techniques in networks to detect anomalous user behavior. Valuable intelligence can be derived by profiling, fusing and mining message content, traffic patterns or IT activity.

Psychological profiling and linguistic analysis are still in their infancy but offer huge potential for the future. Privacy of course is an overriding issue, but security solutions can be devised to contain the risks for many applications. Ignorance of privacy considerations is a bigger problem, as demonstrated by the recent decision by U.S. Homeland Security to scrap an ambitious $42 million antiterrorism data-mining tool after investigators found it was being tested with information about real people without adequate safeguards.

Another major security concern is lack of consistency in enforcing "acceptable use" policy. Most of these policies are badly written, out of date and poorly communicated. We can fix the latter problems with a bit of effort, but enforcement requires security technology to identify, log and block illegal or inappropriate use of services. This can only be achieved in real-time at the network level. As time goes by, it will be a growing challenge for all organizations.

Related Content

Network gateways are a vital source of security intelligence because they see failed or blocked transactions, providing a unique insight into attempted attacks. This is an important area because we know that behind every major incident there are dozens of minor incidents and hundreds of near misses. Smart security is about learning from the little events to prevent the bigger ones. Gateways also provide a valuable point at which unauthorized transfers of confidential information can be detected and blocked. Following the spate of high profile data breaches, this is becoming a key objective for many organizations.

You can deploy encryption in networks or endpoints. In either case it can be a mixed blessing. Encryption protects data passing across hostile networks, but can be a barrier to content analysis. (Read about IBM's massive data encryption project.)

Although encryption use continues to grow, there will always be plenty of cases where endpoints and applications need to communicate "in the clear". In fact there is a trend for end systems to de-fragment into networks of smaller devices, often with no encryption capability. We've gone from mainframes to personal-area networks. Eventually we'll get to smart dust and

nanotechnology. Network security will be vital to maintaining system control.

The future of network security might be far from clear-cut. One thing is clear - it will certainly be richer and more sophisticated than we've seen so far. Determining how to plan for a business environment in which everyone is connected and security expectations are high is not trivial. We all have to do it.

Following are 10 questions to ask yourself when determining your own future security architecture.

1. Can you harden your critical legacy applications to operate across hostile open networks?
2. Should you aim to secure your wireless networks?
3. What is the most appropriate strategy for encrypting enterprise and third-party communications?
4. Does your use of encryption present a potential entry point for malware or inappropriate content?
5. How can you best enforce the "acceptable-use" policy?
6. What is the best strategy for enterprise identity management?
7. How do you plan to control third-party users?
8. Should you block or simply alert on suspected intrusions?
9. Should intrusion-prevention systems be sited on hosts or in networks?
10. Should antimalware defenses be incorporated into clients or networks?

Lacey is founder and honorary member of the Jericho Forum, an organization pushing for innovation in e-commerce security. Lacey's background includes two decades working in chief information security officer positions at the U.K. Foreign Office, Royal Dutch/Shell Group and the Royal Mail Group.

All contents copyright 1995-2008 Network World, Inc. http://www.networkworld.com