

Network Security Review

What is security? Security is being “free from risk of loss”. Security is also the “measures taken to guard against espionage or sabotage, crime, attack, or escape”.

When looking at data networks, these definitions of security hold true. You basically want to protect yourself from unauthorized access to business critical applications, data, and resources. But security comes with a price as well. The trick is balancing the cost of providing the security with the cost of recovery if a threat were to strike you.

The only way to be completely “free from risk of loss” in the data network is to never connect a machine that contains critical data to any other machine. Keep it stand-alone. However, in today’s world of anytime/anywhere access, this is not possible. Critical data typically needs to be accessed by more than one person, so the best that can be done is allowing access to those who are authorized and denying access to those who are not.

There are a few key things to remember when talking about data and network security, as well as security in general:

Security is a process, not a solution. You will never come to the point when you can say, “We are totally secure now.” New exploits are devised every day. Security measures need to be adjusted in order to accommodate the new exploits. Your security needs today will be different from your security needs tomorrow.

Security is not a single barrier, but a series of layers. Because you want to allow limited access to critical resources, a layered approach to securing those resources is necessary. Having just one deterrent may stop a few people, but the majority will try and find away around it. Having several deterrents makes it much harder for people to access resources if they are not explicitly allowed.

Given enough time and resources, any “secured” resource can be exploited and accessed. That brings you to the cost of securing the resource as opposed to the cost of

losing it. Remember, cost can mean many things, including man-hours, replacement time, physical assets, reputation, etc.

Someone needs to be watching for security breaches. If no one is checking to see if the security measures are working, you will never know if you have been attacked. Someone needs to be looking at the logs, checking the systems, making sure access is granted to those who need it and denied to those who don’t. Security will do nothing for you if it is not monitored properly.

You need to understand what you are securing, and whom you are securing it from. If you don’t know what you are trying to protect, how can you put a value on it, and justify the cost of securing it? Equally, if you don’t know whom you are protecting it from, how will you determine who has legitimate access?

As you start looking at your security, you need to keep these items in mind. There is a delicate balance to security, and it is different in each case. Those who make decisions about security need to understand these concepts in order to provide the protection and security desired, whether it is the technical staff, the management team or the CEO.

Trusted Network Solutions can help with this process...

Proposal

Trusted Network Solutions can assist you with performing a Network Security Review. We begin the process of securing your network by:

- Reviewing “Acceptable Use Policies”
- Analyzing the network architecture
- Validating firewall rules
- Verifying users and groups
- Checking server configuration
- Performing vulnerability assessments
- Identifying network access points
- Providing documentation about findings

Please contact a TNS account executive for a proposal customized to fit your business needs.