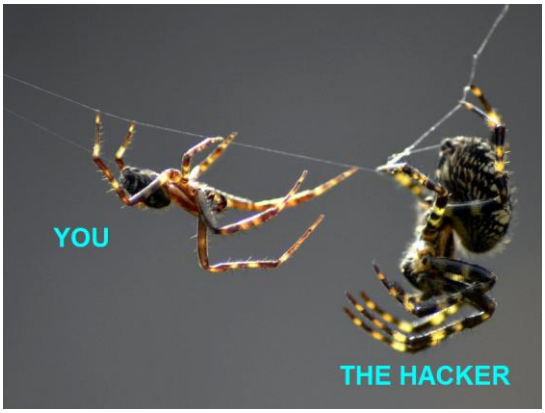
COMMONd
We help organizations do more for less

Network Security – An Oxymoron?

Let's just get it out: There is NO network that is 100% secured…..Well: Unless the network is powered down AND unplugged from the power grid!



Now that we have the answer, should we just give up and go back to paper and fax machines?

That might be an option, but is it possible? Not really… So what should we do? Should we bury our heads in the sand and hope for the best? Or should we spend an obscene amount of cash and hire more security analysts with binders full of certificates to better secure our network?

Before we get there, let's take a step back, look at the "ABCs" and be reasonable.
We cannot argue with reasonable; we like reasonable.
What are the "ABCs," and what do we do?

a. Know your stuff
b. Apply best practices
c. Remember that best practices are only best practices when they are appropriate and are adapted to your own environment

What the heck do I need to know? Where do I start? We need to know that we have to protect the confidentiality of our info, we have to keep the integrity of the info intact, and the data needs to be available when we need it: This is CIA

What are best practices? Prepare + Policy + Prevention = Best practices

Without a sound security policy, the availability of your network will be compromised. The policy should begin with assessing the risk to the network and building a remediation plan. Binders of policies on the shelf collecting dust will do more harm than good. The policies should be reasonable, appropriate, and have the ability to adapt to lessons learned.

Prior to implementing a security policy, you must do the following:

1. Learn about the skillsets of your team: You should question anyone on your team who tells you that the network is OK and that they have it under control.
2. Conduct a risk analysis to identity the risks to you network, network resources, and data. This is the least expensive and the most effective prevention. It is a heck of a lot cheaper to prevent a breach than to lose your reputation, your clients, and/or your job.
3. Be proactive: Get involved and stay involved with what is going on inside the hackers' minds

Layered security and defense-in-depth is an absolute must. In short, the idea is an obvious one: Any single defense is flawed, and the most certain way to find the flaws is to be compromised by an attack. So a series of different defenses should each be used to cover the gaps in the others' protective abilities.

Defense-in-depth will allow you to handle such concerns as:

1. Authentication - Authorization - Accounting
2. Disaster recovery and High Availability for your data
3. Prepare and practice forensic preservation just in case we need to "dig"

For a complimentary Security Pen Test Valued at $3,000.00, contact:
Jeff Maerschalk (720) 320-1890 or
Jeannine Horan (303) 521-4044