

## RE: Securing a Local Network

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-04/0184.html>

---

**From:** Halverson, Chris ([chris.halverson\\_at\\_encana.com](mailto:chris.halverson_at_encana.com))

**Date:** 04/14/04

To: 'John Roberts' <[roberts@tridecap.com](mailto:roberts@tridecap.com)>

Date: Wed, 14 Apr 2004 14:41:41 -0600

1. Show the Management of your company the insecurity of the Peer to Peer setup and discuss what risks are they willing to accept.

Ex. Computer with the financial data's hard drive crashes, discuss length of time that it would take to get that data back up and running.

Ex.2 Virus with payload enters network and causes all the machines to crash and productivity is lost for the day. What do all these things mean to them???

2. Plan, plan, plan. Design three alternate solutions for them a bronze, silver, and Gold solution. All with price tag's associated to them.

2a. Make the bronze least expensive solution, with only a few components per year,

the silver the preferred method for yourself to administer, and the gold the Cadillac of setups, planning for enormous growth from the company (50 + users in 2 years)

All of these should contain an outline of what the pros, cons, and potential risks associated to them.

Things to consider in the plans:

-Make sure that centralized server managed AV solution and if possible a gateway AV solution as well. This should be at the top of the list for the infrastructure upgrade.

-Look to securing the perimeter, test the reliability of the Firewall with some scanning software and looking through the vulnerabilities list for your specific product. If this is a little Linksys Packet Filtering Firewall look maybe to a Linux FW (ex. IPCOP, smoothwall or netfilter)

-Plan your Authentication factors. Windows Active Directory, Samba/SMB Linux Folder permissions, or keep the peer to peer (highly not recommended)

-Internal Training for the users

-Time for setup

-Support for the products that you may purchase.

-Cost of getting the web server and the mail server internally versus having it hosted externally.

-Make sure anything that is accessible from the internet should not be internal to the rest of your network.

-Always account for your time for everything...

-Plan for future growth, and upgrade time frames (don't expect to have all

## SecurityFocus BASICS: RE: Securing a Local Network

the things done in the next month, have a two to three year plan)

- Ensure milestones and expected time of completion.
- Include restore times for any possible failure or incident

Personal Recommendation:

For your situation I would look at MS small business server 2003 (caveat : this product only goes up to 50 user licenses)

- Utilize the Domain Services and the Exchange features of this product ONLY.
- Pick up Xeon or Opteron processor based machine with minimum 1 Gb of ram and redundant disk storage. (Use easily available parts or Name Branded Products and have spare parts in case)
- Have a nightly backup procedure using tape and/or digital backup media and safe offsite storage of this backup medium.
- Get a Cisco 1721 series Router using the FW inspection module with two WICS to have a DMZ for external based services. Mail Front End, web server, and IDS
- Use an older box for Intrusion Detection on the internal network as well.
- Documentation of every step that you took to install and setup this new configuration
- good logging facilities.

There is a lot more you could do and I am sure you will hear numerous solutions. Take them with a grain of salt and make sure the solution will be easy for you to manage...

---- to the remainder of security gurus on the list ----

I have been looking at a good way for windows clients to authenticate to a directory such as Active Directory within Linux and I have yet to find anything of value. There is PAM but I find it is not as robust as AD :(

Does anyone have some sort of solution for this?

---

-----Original Message-----

From: John Roberts  
Sent: Tuesday, April 13, 2004 11:17 AM  
To: security-basics@securityfocus.com  
Subject: Securing a Local Network

I started working as a sys admin at a small company (about 15 people) and they are starting to think it's time to upgrade their network. Right now it's just 20 computers, running a mix of xp and 2000 on a local network, sharing files, with almost no anti virus and the only protection from the outside world is the NAT that the routers perform.

I've tried to get the to upgrade to a domain, add a file server for backup, get some office wide virus protection and maybe even take our email in house, but they've balked at the price to setup a legit windows domain. The main goals are access control on the local network and virus / worm

RE: Securing a Local Network

## SecurityFocus BASICS: RE: Securing a Local Network

protection. I'm suggesting a Windows domain controller to enforce access control and then an centralized anti-virus product. Is this enough, and are there other (easier, cheaper, more effective ways) to make sure that only the people who need to can access the financial records, the computer people can access the all computers when they need to, and some user decides to download a cute little program won't destroy the whole network with a virus.

Is a linux domain controller a solution, considering everything else in house is windows? Is an anti-virus solution at the gateway better than an anti-virus solution on each desktop? Basically, what's a good way to set up a solid base of network security, which can then be expanded on?

John Roberts

---

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:  
[http://www.infosecinstitute.com/courses/ethical\\_hacking\\_training.html](http://www.infosecinstitute.com/courses/ethical_hacking_training.html)

---

---

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:  
[http://www.infosecinstitute.com/courses/ethical\\_hacking\\_training.html](http://www.infosecinstitute.com/courses/ethical_hacking_training.html)

---