

Re: Oh Dear, Where to start?!

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-06/0851.html>

From: Chris Berry (*compjma_at_hotmail.com*)

Date: 06/25/03

To: security-basics@securityfocus.com

Date: Wed, 25 Jun 2003 12:47:36 -0700

>From: Steve Frank <stevefrankrit@yahoo.com>
>Hey everyone,
>
>Ok... I am in a bit of a jam here and I was hoping to
>get some feedback from some of you with appropriate
>experience in the field of network security and policy
>development.
>
>I am an senior at RIT studying (essentially) systems
>administration. My main focus and priority has been
>computer security and policy development. I recently
>took a internship with a small government office
>helping out with computer administration tasks. Upon
>arrival, I decided it would be fun to do a windows
>update to see what sort of things would come up for my
>PC. Low and behold, there were over 40 critical
>updates, driver updates, and recommended updates.
>
>Right off the bat this triggered the feeling that
>there was absolutely no security or update plans in
>place at this particular organization. I quickly
>addressed the issue, and have been working to draft a
>comprehensive security policy and implement technical
>controls.
>
>What I need advice on is the following: If you were
>introduced to a mixed network (literally all versions
>of windows since 3.1 and mac systems) that have no
>updates, backups, or patches installed... connected to
>a network with only a basic NAT table and no other
>security... with not even anti-virus software
>enabled... with no user policies or disaster plans in
>place... with unprotected netbios shares everywhere...
>where would you start the process of building some
>sort of security solution?
>

SecurityFocus BASICS: Re: Oh Dear, Where to start?!

*>I mean, I've seen passwords on monitors, shared
>accounts, open public ports (even the wiring cabinet
>was unlocked in plain view of passbys to the
>building). I've been tasked with creating the security
>policies relating to internet use, network and phone
>use, passwords, physical security, backup/disaster
>plans, antivirus, incident response, email
>use/protection, and whatever else needs done. This
>wouldnt be so bad normally I guess, but there is
>virtually no budget allocated to help for this project
>and I have approximately 3 months to do it. To make
>matters worse, I am also responsible for systems
>admin, network admin, tech support, programming, and
>whatever other tasks may need to be done in the
>meantime.
>
>So basically, if you had to start from nothing, where
>would you start first? What would you consider to be
>the most important things to be implemented? I am
>literally working from ground zero here... heh!*

(I don't know much about macs so I'm leaving them out)

This was pretty much my exact situation when I started here. First you have to acknowledge the fact that your three month time limit means this is an emergency, and deal with things on that footing. Forget trying to write up all the policies first, you're the only one dealing with this, so you need to DO SOMETHING, you can write about it once things calm down a bit. Here is the first things I would do, in order:

- 1) Setup a firewall, since you have a low budget and are pressed for time, I recommend IPCOP, you should be able to have it up and running on an older box in less than 30 minutes even if you're not big on Linux knowledge.
- 2) Install anti-virus software. If you have any budget at all this is where I'd spend it, get Norton corporate and install it everywhere then run a virus sweep. There are a number of free scanners, but nearly all of them (including AVG) are not legal to run in a networked environment.
- 3) Use Active Directory to deploy SP3 to all of your machines automatically, then go around and configure the automatic updates feature to run nightly and auto-install critical updates. (Later on you'll want to switch over to using an SUS server, but for now this is good enough)
- 4) Configure the security policy for passwords with min length, complexity requirements, history, etc. then force a password change on everyone on the system.
- 5) Set up groups and assign users to them (don't worry about getting them perfect, you'll have to tune this later) then start restricting access based on membership. Especially check the membership of all admin groups, often times they'll have like 22 domain admins or some other silly thing.
- 6) Download a copy of spybotsd, deploy it, update it, and scan all of your machines.
- 7) Get some locks installed for physical security of the server room and

Re: Oh Dear, Where to start?!

SecurityFocus BASICS: Re: Oh Dear, Where to start?!

wiring closets.

8) Get a policy established that prohibits having your password on a sticky note, in your desk etc., then do a sweep through the office looking for them. (get management approval first)

9) Do a hardware and software inventory to see what you've got, and get started on making sure you're license compliant.

10) Audit your servers and turn off unnecessary services.

Ok, that's the worst stuff, once you've finished all that you can slow down and start working on a more formal implementation and tightening things up further.

Chris Berry
compjma@hotmail.com
Systems Administrator
JM Associates

"Within every man beats a heart of darkness." --The Shadow

Add photos to your e-mail with MSN 8. Get 2 months FREE*.

<http://join.msn.com/?page=features/featuredemail>

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!
The Gartner Group just put Neoteris in the top of its Magic Quadrant,
while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug-n-play secure remote access in
about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>
