

RE: in-to-out security

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-03/msg00390.html>

- *From:* "Beauford, Jason" <jbeauford@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 28 Mar 2006 11:28:52 -0500
-

Joe,

1.) Acceptable Usage Policies are the very first step and are ABSOLUTELY required. As you have seen already, the toughest part is getting Upper Management approval.

2.) Gaining UM approval is a common topic of discussion. Generate some sort of Risk Assessment. Evaluate the costs associated with an "incident". Evaluate and demonstrate (if possible) the kinds of problems you are seeing on the network. Use laymen terms rather than techie jargon to explain. UM needs to know exactly whats going on in words they can understand.

Use available tools to start building your case. NTOP can monitor traffic flows on your network. If you can show that certain traffic is being passed on the network and that there is a risk associated with it (TORRENT / P2P traffic for example risks exposure of sensitive corporate documents) then you may be able to convince them.

3) There are plenty of GPL and Commercial products available to monitor and limit traffic flows. You'll need to specifically identify what it is you want to do and evaluate the solutions for your organization.

4.) If you do not implement an Acceptable Usage Policy and fail to inform your employees that network traffic may be monitored, you open yourself up to legal liabilities. The company should consult a lawyer to help finalize such policies and help identify any legal obligations.

-JMB

| -----Original Message-----

| From: Joe George [<mailto:j.george@xxxxxxxxxxxxxxxxxxxx>]

| Sent: Tuesday, March 28, 2006 9:33 AM

| To: security-basics@xxxxxxxxxxxxxxxxxxxx

| Subject: in-to-out security

|

| Dear all,

|
| I hope you're all doing well. A colleague of mine
| does technical support for some charities on the
| side. One of his clients is a person who is the CTO
| of a 400+ person, non-profit organization. This CTO
| asked my colleague what was the best way to (a
| particular application or training method) to get
| his 400+ staff in-line and keep them from doing
| inappropriate things on the network such as
| downloading rogue applications, and inadvertently
| installing apps which can attack the network and
| other networks. He's looking for an in-to-out solution.
| This CTO feels he and his team would be able to
| secure the network from intrusion from outside rogue
| users by implementing necessary firewall, IDS, etc.
| I suggested to my colleague that this gentleman can
| not adequately secure external/internal intrusion
| and attacks without implementing an acceptable use
| or some kind of written policy with the assistance
| of his HR department. I informed him that end-users
| should have the right to know that their activity is
| being monitored by the IT staff (which is what I
| presumed he meant by an application/training method
| to keep his staff in-line). This CTO fellow, feels
| that any kind of policy is not a viable option. I
| told my colleague a written policy will protect the
| organization and the employees and allow the
| security team to build and design a security
| countermeasures, not to mention get the best use of
| expensive security appliances. Besides rogue
| applications, I mentioned that other issues such as
| disgruntled employees, corporate espionage,
| maintaining data and company integrity are just a
| few reasons to start off with written policy. My
| colleague mentioned that his CTO client is not
| uninformed, but rather too scared to bring up a very
| controversial solution as written policy to his
| superiors and the end-users. My questions to you are these:

- | 1. Was I right to suggest this rather than help my
| colleague look
| for an app/training solution?
- | 2. How would you convince an obviously passive CTO
| to do the right
| thing?
- | 3. If such an application/training exists, can you suggest
| something?
- | 4. Is it legal to implement user-monitoring
| without informing the
| staff? This is where I think policy

|
| Thanks in advance.
|

| Take it easy,
|

| Joe
|

| EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE –

| ONLINE The Norwich University program offers
| unparalleled Infosec management education and the
| case study affords you unmatched consulting experience.

| Tailor your education to your own professional goals
| with degree customizations including Emergency
| Management, Business Continuity Planning, Computer
| Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The Norwich University program offers unparalleled Infosec management
education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree
customizations including Emergency Management, Business Continuity Planning,
Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>
