

Re: [fw-wiz] Security and Audit Policy

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-11/0082.html>

From: gmx (carpathin.wolf_at_gmx.net)

Date: 11/27/04

To: Servie Platon <servie_tech@yahoo.com>

Date: Sat, 27 Nov 2004 12:07:14 +0100

Hello Servie,

I will try to give you my opinion, maybe also between the lines..

Sunday, November 7, 2004, 3:38:55 PM, you wrote:

<=====Original message text=====

SP> -----BEGIN PGP SIGNED MESSAGE-----

SP> Hash: SHA1

SP> Hi Security Gurus,

SP> When I took over as Sys Ad for this company, I found

SP> out there

SP> are no security and audit policies in place. I have no

SP> way means

SP> of getting in touch with the previous guy.

Thats a har work for you... but not impossible

SP> Since I have to start from scratch and document

SP> everything

SP> regarding this network. I feel that this group would

SP> be in the

SP> best position to give some suggestions as to what I

SP> should do or

SP> the manner of solving the problem.

Documenting is a good start, take also a look for checklists (google)

and be cofidential with www.cert.org . There you might also find some good suggestions.

SP> I have already done the following steps:

SP> 1. Enabled Firewall rules on the network and with

SP> Win32 clients;

SP> 2. Installed Anti Virus Software for the network and

SP> enabled

SP> automatic updates;

Firewall-Wizards: Re: [fw-wiz] Security and Audit Policy

SP> 3. Enforced User Permissions for most users; (dilemma)

SP> 4. Disabled M\$ Outlook and IE and replaced these with

SP> Mozilla

SP> Thunderbird and Firefox.

Good start point... but how do the email clients connect ?

Do you have a central mailserver which the clients are connecting ?

SP> Problems:

SP> 1. I don't know how to keep track of their browsing

SP> patterns,

SP> some users have intermediate to advanced browsing

SP> skills which

SP> they can conceal where they have visited such as maybe

SP> porn

SP> sites and the like. How do I prove my suspicion and

SP> stop them

SP> from doing this? I am afraid that by doing so, our

SP> network may

SP> be trojaned or may have been infected with spyware or

SP> may be a

SP> zombie now?

Well... i cant say if you are 100% allowed to check their trafic, but you can install some tools and see the browsing behaviour (MS SBS ISA does have such tool integrated), i am sure you can find some cmpatible tools also in the web.

SP> 2. I wanted to enforce strict user permissions, but my

SP> dilemma

SP> would be, bosses or managers take it against me or

SP> anyone

SP> restricting on what they could or not do on their

SP> machine. To

SP> make a concrete example, I could do an audit policy

SP> for all

SP> users with less rights to install programs and the

SP> like but some

SP> of them, listen to radio, download .exe files or

SP> shareware

SP> without my knowledge.

Thats a wrong way... you started good, but you missed the human component.

SP> If I enforce this restrictive permissions, they get

SP> back on me.

SP> If I don't, I am afraid the network is considerably

SP> slows down

SP> and I think, some machines may be a compromised

SP> already unless

SP> the bandwidth is being used up by the users. How do I

SP> catch them

Re: [fw-wiz] Security and Audit Policy

Firewall-Wizards: Re: [fw-wiz] Security and Audit Policy

SP> accessing forbidden sites and how do I stop them from
SP> doing such
SP> and how do I make them with less capacity without them
SP> getting
SP> furious?

Easy : You dont tell them what to do, you ask them what they want.
You ask about their fears... the users must have the feeling that the
admin is the one who is on their side, not against them. Use your
knowledge to explain the management what costs can arise in case of an
intrusion, and why you must solve it taht way.
You can do some small seminars, and explain to the users about seafe
browsing, its all up to you, but as an admin, you must get the company
on your side.. thats what the harder part for an admin is.

SP> 3. Though, I have setup and installed Mozilla
SP> Thunderbird and
SP> Firefox in each client PCs, most of them still use M\$
SP> Outlook
SP> and IE. How do I justify and convince them not to use
SP> this
SP> because of security loopholes and problems? Some are
SP> so used to
SP> Outlook and IE that they don't want change.

Explain them that during some seminars, explain also why you dont
recommend outlook, but you must have the management 'behind you' ,
because you cannot assert any policy or guidelines, without the
approval and help/cooperation of the management.

SP> Any suggestions, on how to make it less of a burden to
SP> administer this network of 12 clients would be
SP> appreciated.
I hope i could give you a few sugestions.

SP> Thanks very much.

SP> -----BEGIN PGP SIGNATURE-----
SP> Version: GnuPG v1.3.92 (MingW32) – GPGshell v3.23

SP> iD8DBQFBjjNBuG3YFhFbIMkRAiXDAKDT0ywwBwfM7qi1VS5HOFPOi3LhkACg6eFg
SP> FR5U6VihJqU4Otz7bYyQh9s=
SP> =poMj
SP> -----END PGP SIGNATURE-----

SP> =====
SP> Sincerely,
SP> Servie Platon

SP> _____
SP> Do you Yahoo!?
SP> Check out the new Yahoo! Front Page.

Re: [fw-wiz] Security and Audit Policy

Firewall-Wizards: Re: [fw-wiz] Security and Audit Policy

SP> www.yahoo.com

SP> _____

SP> firewall-wizards mailing list

SP> firewall-wizards@honor.icsalabs.com

SP> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

<=====End of original message text=====

--

Best regards,
gmx

<mailto:carpathin.wolf@gmx.net>

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>