

Re: Network + AD = Tighten Security

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-04/0655.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 04/14/04

Date: Wed, 14 Apr 2004 17:30:53 GMT

Thanks Tim.

Sometimes I get carried away. Sorry. ---- Steve

"Tim" <Tim@NoSpam.com> wrote in message news:c5is3k\$84a\$1@lust.ihug.co.nz...

> *Dear Steve,*

>

> *The Enter key can be used to break up long sentences into things called paragraphs.*

>

> *For us mortals, it improves readability enormously and assists us in comprehending your valuable contributions.*

>

> *Regards...*

> *- Tim*

>

> *"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message*

> *news:_IZec.30740\$wP1.85975@attbi_s54...*

>> *Well there is a lot that can be done depending on how you want to balance security*

>> *and functionality.*

>>

>> *I would be careful about setting your lockout threshold too low. MS recommends*

>> *minimum of ten which will protect your network fine with complex passwords. In*

>> *addition I would enable auditing of logon events on the domain controller and any*

>> *servers being sure to increase the default log size substantially. If at all possible*

>> *do not let users be local administrators on their machines nor power users and the*

>> *default ntfs permissions on the root/drive folder is too permissive in W2K where you*

>> *want the everyone group to have no more than read/list/execute. keep in mind that*

>> *newly created shares will give everyone full control which you want to usually*

microsoft.public.win2000.security: Re: Network + AD = Tighten Security

> > change. Assuming internet access I would also look into configuring the
> web content
> > zones of your users to have minimum settings and taking advantage of the
> trusted web
> > content zone to place "authorized" sites that are know to be safe. Of
> course you will
> > have to prevent users from having access to IE settings to undo what you
> have done.
> > There is a setting in IE/advance to disable on demand install of third
> party addons
> > which I would disable, though I do not know of a way to do that through GP
> > unfortunately. If you do not want users to install unauthorized software
> it will help
> > to enter setup.exe and install.exe to the list of disallowed Windows
> applications in
> > user configuration/administrative templates/system. A firewall with a
> default block
> > all outbound rule and then the allowed exceptions can keep users from
> running
> > unauthorized internet programs such as chat and file swapping. Also keep
> in mind that
> > a malicious user can reset the local administrator password if they are
> able to boot
> > their computer from a cdrom, floppy, or other device. Therefore you will
> want to
> > configure the computers to boot only from the hard drive and password
> protect the
> > cmos settings and have locking computer cases if posible to prevent them
> from
> > resetting the cmos via jumper. If you do not need usb [pen drives]then
> diable that in
> > cmos and use GP to diable autorun of cdroms. The domain controller must be
> physically
> > secured to some degree even it is just a real heavy duty case with access
> to ports
> > and drives blocked. You should also run Microsoft Baseline Security
> Analyzer at least
> > on your domain controller and other servers. For instance in a default
> install of any
> > W2K server IIS is enabled which should be disabled or unistalled if not
> needed. That
> > should give you a good start. --- Steve
> >
> > <http://support.microsoft.com/default.aspx?scid=kb;en-us:323525>
> > <http://mvps.org/winhelp2002/unwanted.htm> -- tips on securing IE settings.
> >
> > <http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/05sconfig.msp>
> > msp --- more
> > advanced security options.
> > <http://www.microsoft.com/technet/security/tools/mbsahome.msp>
> >

microsoft.public.win2000.security: Re: Network + AD = Tighten Security

> > *"NewToAdminSide" <anonymous@discussions.microsoft.com> wrote in message
> > news:1013EA9E-3AAE-45E5-A3FE-AF368FD0C299@microsoft.com...
> > > We are trying to tighten up our security here and was wondering what
> else could be
> > done through AD besides:
> > > 1. Workstation lock down after idle for 20 min
> > > 2. We changed our password policy to include a lower threshold, lower
> > > lockout and
> > > password complexity
> > > 3. We changed our Administrator passwords
> > > 4. We've added all updates and patches.
> > >
> > > Is there anything else we can add? We are a small biz with about 55
> users.
> > >
> > > Thanks all!
> >
> >
>
>*