

Re: Web App Security Model.

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-03/msg00007.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Thu, 1 Mar 2007 00:33:44 -0700
-

"Lincoln De Kalb" <lincoln.dekalb@xxxxxxxxxxx> wrote in message news:eq%23LCZ8WHHA.4624@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Thanks for the information.

So basically just follow standard procedure for locking down IIS / Websserver etc and I should be OK.

OK if the web application itself is well designed / implemented and the SQL permissions are correctly restrictive (so worse case the allowed database is extent of what is at risk on the SQL server). Also, if Windows integrated domain account is used for the SQL access (i.e. trusted connection)

then if the web app can be exploited then potentially anything in the domain is at risk to the extent that the domain account has grants (ex. if it is in Domain Users, if there are grants to Authenticated Users, etc.) and that the network connection between the IIS box and the SQL box can get to other locations (such as certainly to the DCs).

Again, very much depends on the quality of the web application(s).

Because of the authentication needed I'll be in the Active Directory domain. The app will be connecting to a SQL 2005 server in the domain. I'm thinking about putting it in it's own sub-domain but the additional costs of servers for DC's might be prohibitive.

Not just high cost, but it probably would not provide much gain.

Thanks again.

no problem

Re: Web App Security Model.

"Roger Abell [MVP]" <mvpNoSpam@xxxxxxx> wrote in message
news:%23vX9IF0WHHA.4860@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Some would say it is better to have those machines, latched down to tcp 80, 443 as you say, sitting outside compared to inside in the circumstance you describe.

You have not indicated how the machines are with regard to AD, any domains, etc. database accesses, backup access, etc..

If these machines are standalone the threats posed by them are significantly different from if not, obviously, but much also depends on how inconvenient administrative / backup / etc access is if they are standalone (generally more convenient is more risk)

Anyway, very very much depends on the quality of the aspx applications / implementation and whether their design has been done with security (of your whole infrastructure) in mind.

There is some guidance at
<http://www.microsoft.com/technet/security/guidance/default.msp>
and IIRC more in msdn2

Roger
"Lincoln De Kalb" <lincoln.dekalb@xxxxxxxxxxx> wrote in message
news:e3jok4uWHHA.392@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hey all,

I'm not really looking for an answer, i'm looking for pointers on where to look.

My company wants to have a few Windows Servers running web app's (ASPX based primarily) available externally. They will be behind a firewall with strict rules (like 80, 8080, 443) etc....

For the time being there wont be a Firewall between the servers and the primary network, so we aren't in a DMZ type environment.

I'm struggling to find any information on technet, windowssecurity.com, techrepublic etc etc. on best practices or thigns to consider for this type of environment. I really wouldn't have thought it that different to what most people would set up.

Re: Web App Security Model.

So if you can point me in the right direction, that would be superb. Or maybe i'm missing something so fundamental that it's a no brainer and hence no documentation.

Ta heaps.
Lincoln