

Re: Securing SQL

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-11/0247.html>

From: karl levinson, mvp (levinson_k_at_despammed.com)

Date: 11/24/05

Date: Thu, 24 Nov 2005 08:46:27 -0500

"Bad Beagle" <maxwelli@nospam.postalias> wrote in message news:uCxmBEE8FHA.444@TK2MSFTNGP11.phx.gbl...
>I would like to know what the suggestions are for designing a secure
>solution for Windows servers and SQL. I have a Windows 2000 server that is
>my web server – this server is in the dmz. This server has pages that
>access a SQL server. The SQL server hosts a database that is used both
>internally and externally and needs to be updated by someone internal. My
>question is where this SQL server should be placed – on the lan and do file
>replication or in the dmz and open up the firewall for sql traffic.

I would suggest any solution that prevents the servers in the DMZ from opening inbound connections into your internal LAN and requires that connections be established from your LAN to the DMZ. Having two SQL servers, one on the LAN, one in the DMZ, that are synchronized by the server on the LAN sounds most secure, but then you want to make sure the synchronization works for you and does not cause unacceptable data discrepancies.

A cheaper solution that is probably secure enough would be to have the one SQL server in the DMZ — preferably a second DMZ for example using an additional network interface in your firewall or an additional inexpensive firewall like the www.netscreen.com "5" series, so that the SQL server is firewalled from both the LAN and the web server — AND only allow connections from the LAN to the SQL server.

Note that using IPSec authentication and encryption does not make it safe to permit connections from the DMZ web server to a server on your LAN, because attackers may be able to use that connection.