

Re: Protecting database from administrators

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2004-04/0413.html>

From: Stephen Dybing [MSFT] (stephd_at_online.microsoft.com)

Date: 04/27/04

Date: Tue, 27 Apr 2004 07:04:51 -0700

I'd just like to throw my two cents in the ring behind Neil. There is absolutely nothing preventing you from mentioning competitive products in this newsgroup. It's a public space that Microsoft hosts, not owns. We would never remove a post because it mentions a competitive product. We may remove a post if it contains spam, pornography, direct personal attacks, or similar, but never simply because it mentions a competitor. This is a public space for you to share your knowledge. Please do.

--

Sincerely,

Stephen Dybing

This posting is provided "AS IS" with no warranties, and confers no rights.

"Neil Pike" <neilpike@compuserve.com> wrote in message

news:VA.000061e7.01dc2cb6@compuserve.com...

> Andre,

>

> > In transit means legally or illegally. If the DB is removed illegally and

> > there is no encryption while at rest it must still be secure. We do not

> > want to use separate encryption utilities to achieve this. These should be

> > part of the DB itself.

>

> It would certainly be nice if SQL Server provided more encryption facilities,

> but not many people would use them. Oracle and DB/2 have a level of encryption

> facilities, but I've not seen them actually used anywhere yet! (Note that's

> just my own experience). Almost all the "proper" encryption I've seen done

> with DBMS's so far, has been done at the application level, often in

> conjunction with a hardware encryption card, to encrypt/decrypt sensitive data

> fields outside the control of the dbms.

>

> > It is very clear that you are unaware of DBMS that

> > are not linked to OS security.

>

> Please enlighten us all then - this is a forum for sharing information.

>

> > All the security MS has offered is weak.

> > Let us take one simple example. You refer to EFS. This is only applicable

> > if the DB is lying on an NTFS segment. If it is attached to SQL Server

microsoft.public.sqlserver.security: Re: Protecting database from administrators

on
> > FAT32 (e.g. Windows 98) the security is removed as FAT32 does not support
> > EFS.
>
> Quite correct. EFS is one possible option worth considering when looking at a
> secure solution. There's no "magic" answer that fits all requirements.
If
> there was then there would only be one dbms product out there and one "security
> solution".
>
> > We have solved our problem by not using MSSQL. We have connected with
> > other vendors that supply SQL technology that meets our requirements and is
> > not dependent on the OS at all. I suggest you do some more research on this
> > matter. We have been digging around for well on one year now - specifically
> > on the security aspects. A cursory bit of research on your part is all that
> > is required. It is unethical to mention other vendors on this forum so we
> > will refrain from doing so.
>
> Unethical? In what way? Anyone here is perfectly free to discuss the pro's
> and con's of any and all dbms's. Obviously the majority of people here use SQL
> Server, but most people work in multi-vendor environments using many products
> and technologies. Any and all opinions are always welcome. Hard facts are
> even more welcome.
>
> Why not share the research you've done by letting us know what product(s)
> you've used, what the security features are, and how these compare to what
> other products, such as Oracle, DB/2, SQL Server, Sybase and anything else,
> offer.
>
> Neil Pike MVP/MCSE. Protech Computing Ltd
> Reply here - no email
> SQL FAQ (484 entries) see
> <http://forumsb.compuServe.com/qvforums/UK/default.asp?SRV=MSDevApps>
> (faqxxx.zip in lib 7)
> or www.ntfaq.com/Articles/Index.cfm?DepartmentID=800
> or www.sqlserverfaq.com
> or www.mssqlserver.com/faq
>