

Re: No lockout policy... why not?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-05/msg00390.html>

- *From:* "Dave Nickason [SBS MVP]" <gwdibble@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 2 May 2007 14:03:27 -0400
-

The biggest thing that relieves my anxiety about remote access attacks is two-factor authentication. This applies to all of the accounts, not just Administrator. I'm currently using Cryptocard, but a more appropriate SBS-sized solution has been released since I bought Cryptocard. Without the authentication token and PIN, you can't even get to a password prompt to attempt to use a Windows password.

See <http://www.scorpionsoft.com/> or come to Jeff Middleton's NOLA conference to check this out for yourself <http://www.conference2007.sbsmigration.com/>

"kj" <kj@xxxxxxxxxxx> wrote in message
<news:uKrFO5NjHHA.492@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Anna Clark wrote:

Oops! Thanks kj

Seems Anna was napping in class when the subject of Administrator security was discussed. :-)

More research is required. But after a quick review of the literature it is still not clear that disabling and/or renaming THE Administrator account is either a workable solution or will do more than slow down a knowledgeable bad guy.

Of course slowing them down is a valuable objective, but an authenticating firewall ahead of the server, preferably one that logs unsuccessful attempts and can do "lockouts" of its own, with entirely different user id's and passwords would still seem to be the "more secure" solution.

No, there is no one thing that can be done to make you 'secure'. The administrator account is just a primary target. If you audit any of your sites you'll find (or should) at least one other account that if compromised would be a bad thing.

Re: No lockout policy... why not?

All of these are good practices at building depth into the site security. Focusing on the firewall isn't all that should be done. The (US) FBI reports 75% of security breaches are from inside the firewall. Consider for just a moment the new generation of cell phones some of which have built in WiFi. How many of these will be walking in the doors of your sites soon?

--
/kj