Re: Recommended Windows Hosts

Source:
http://www.tech−archive.net/Archive/FrontPage/microsoft.public.frontpage.client/2004−04/2278.html

---

From: Bob (*uctraingNOSPAM_at_ultranet.com*)
Date: 04/11/04

```
Date: Sun, 11 Apr 2004 03:25:07 GMT
```

On Fri, 9 Apr 2004 07:34:41 −0500, "Jim Cheshire"
<contactme@www.jimcoaddins.com> wrote:

>Your comments seem to indicate that you are simply another anti−Microsoft
>zealot.

Nope. I actually like using their software. I have a major
disagreement with their business strategy though and their
resulting architectural problems that lead to unsolvable
problems with their security.

> For example, you say, "While MS is making (at least publicly) an
>attempt to repair security flaws...". In fact, Microsoft IS repairing
>security flaws. Perhaps you can explain how you can publicly repair
>security flaws without doing so internally.

My point is that they are patching a damaged architecture. They will
continue to have problems because of the architectural issue.

> If you've been reading tech
>news over the last few years, you would know that Microsoft is absolutely
>committed to security. You would also know that Windows is the most secure
>operating system available today.

Sorry, but that's not true. Windows is not the "most secure operating
system available today". It can't even isolate applications from
each other, let alone the OS. This causes 95% of their security
related problems. Go check with the US Gov't on what they use for
secure OS's when real security is required. I think you might be
surprised.

>You disagree with me because of your lack of information and you bias.

Sorry but you've made a bad assumption. I'm very informed about
security. I'll suggest that you need to learn something about how a
truly secure operating system works.

> As
>an example of my assertion, there was recently a security hole in Linux that
>allowed someone hitting a Web server to easily elevate their privileges to
>root. It was widely reported. You know how long it took them to fix it? 8
>months! That's just unbelievable, and it's laughable that anyone would
>claim that Windows is less secure than that.

I think you may be mistaken on the specifics of that issue. Trust me,
Linux servers are not wide open with security breeches. However, I
would not claim that they have no holes. They do. It's still a much
more secure environment than MS−Windows will ever be with MS's
business strategy.

>By the time you read of a
>security flaw in Windows, Microsoft has already patched it, and Microsoft is
>the only company that has a very simple and effective way to ensure that
>your OS is always up−to−date.

Simple for you perhaps. Not so simple for my clients with multiple
systems that are Internet isolated for security reasons. However, I
don't disagree that MS is trying to patch the holes. My disagreement
is with the fact that they built a container that can't structurally
hold water... and they continue to patch leaks in it.

>Concerning the parent−pathing issue (../../), for YEARS, Microsoft has
>recommended not allowing parent paths on the Web server. In fact, the IIS
>Lockdown tool (available for a few years itself) disallows this and other
>security holes. It is up to the server administrator to enable parent
>pathing. Most do because they don't want to have to tell developers not to
>rely on parent pathing. Make that choice and the consequences are yours,
>not Microsoft's.

Lockdown came out after this hole. In fact, Lockdown was a reaction to
the repeated problems with the IIS environment. The fact remains, once
again, that this is a *architectural* issue. MS designed it on
purpose. The architecture should prevent this from ever happening. No
request to the web server has any business outside the web server.
Ever. Period. No exceptions. If you want a program on the web server
to access OS features, go through a program on the web server that
has been specifically enabled and secured to allow that to happen.
The exception, not the rule. The reason that this was possible was
MS's lame architectural design.

>Concerning the requirement to have a Windows account in order to be
>authenticated to the Web server, how in the world do you perceive this as a
>security flaw? Your criticism of this approach shows a bit of
>short−sightedness. Do you develop multi−tier Web applications? I don't
>think you do, because if you did, you would realize how critical such a
>system is to a good user−experience. In a multi−tiered environment, I may
>hit five or six different resources that require authentication. You think
>it's actually a good idea to require users to enter their credentials over

>and over and over and over? Worse yet, do you think it's acceptible to
>allow multiple systems to authenticate me by proxy? Microsoft systems don't
>allow that unless you have explicitly configured delegation. Once again, a
>very secure architecture.

It's simple: Web servers are public "holes"
in the security blanket. You do NOT design access to the web server's
public or private resources by giving the user an account with the
potential to access the server itself (and therefore potentially
anything the server can access... can you say "big enough to drive a
bulldozer through [your network]).Instead, you give the user an
account which can only access the web server which is totally
isolated from the system security − not just "restricted"
but truly isolated. When I put an MS server on the public internet
and want to do any sort of public/private access, I now have to grant
NT user accounts to the general public. Wrong, wrong, wrong.

The reason that MS has done as they have is exactly what you've
suggested: to sell solutions to the corporate market with a "one
login", share everything, strategy. This is the part of the
business/architectural problem that I've cited. They want to sell
corporate integration solutions − for them, the security is second
tier. You've hit the nail on the head − this is part of the MS
"hey, we can sell this" strategy and a corresponding "security
can take a back seat" attitude.

It doesn't matter that this is more "convenient" for the corporate
user. It's wrong. This sort of thing is the very reason that MS has
major architectural security issues. However, you can see how it
butts heads against their business strategy. That's the core of the
issue. Congratulations on your arrival.

>To close, I think it's clear to those who think about these matters that
>security holes in Microsoft products (even though they are already patched)
>are more publicized than in other systems simply because of the fact that a
>very high percentage of computers in the world are running Microsoft
>software. If you were a virus or worm writer, would you target a system
>used by single−digit percentages, or would you target systems in use by a
>wide majority of people in the world? I know the answer, and I think you do
>too!

I don't disagree that MS is a larger target. They definitely have the
desktop presence. If we are talking the server market, we have to
realize that MS is less than 50% and they are still a target. However,
the fact remains, as I've said repeatedly, that the problem is
architectural to their business, and thus their system, strategy. They
want to sell software at any cost and a flawed architecture designed
without security concerns is the result.