

Re: Question for the Group

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2007-06/msg01873.html>

- *From:* david20@xxxxxxxxxxxxxxxxxxxx
 - *Date:* Wed, 20 Jun 2007 13:58:43 +0000 (UTC)
-

In article <5dsnecF36dckuU2@xxxxxxxxxxxxxxxxxxxx>, bill@xxxxxxxxxxx (Bill Gunshannon) writes:

In article <f5b5qj\$3c\$1@xxxxxxxxxxxxxxxxxxxx>, david20@xxxxxxxxxxxxxxxxxxxx writes:

In article <f5ardb\$3il\$01\$1@xxxxxxxxxxxxxxxxxxxx>, Michael Kraemer <M.Kraemer@xxxxxx> writes:

AEF schrieb:

Pardon my ignorance, but didn't Apple do the same? What did they do wrong?

Certainly I do not have to repeat PC history here, or ? It was IBM+MS+intel who lay the foundation for PCs dominance in the 1980s. No chance for a small startup like Apple to change that, no marketing could have done that.

They could be happy to stay at a few % of the market, and even for that they will have to work harder and innovate faster than the rest.

Others
advertise
security.
Why not
VMS? Why
not back it
up with
something?
What would
it hurt?

Re: Question for the Group

Nothing, but would it help ?
Everybody claims to be
"secure"
these days. Now if VMS
would have some security
certificate
from NSA or whoever
issues such things, putting
them five notches
above the usual Unix crowd,
that would be something to
brag about.

And those who claim security are doing
better than VMS. So, if VMS
claimed security, it should do better, too, no?

Just think of a guy of those two or three academic
generations
who have left unis without ever having heard about VMS.
For him, these letters would expand to "Video Management
System",
or, as in google.de, to "Verkehrsverbund Mittelsachsen"
which
is a public transport service in eastern germany.
He might read an ad about super-secure VMS, but
on the next page there's an ad about hyper-secure AIX
and on the next page another one touting ultra-secure
Solaris.
Even if he hasn't heard about the latter two, how should he
be able to differentiate ? If there would be some official
certificate rating one high above the others, this would be at
least some differentiator.

OTOH, "security" these
days means to organize your
IT so
that it has minimum cross
section to the evil internet,
rather than the choice of a
particular OS.
Raise a firewall, hide
business critical systems and
important databases etc.

Re: Question for the Group

Which isn't really enough.

These are by far the most important measures,
much more important than the choice of OS.
I think most security paranoid will tell you so.

No you need multiple security layers. Firewalls cannot protect you from attacks through ports you leave open to enable the server to do it's business. Eg If you are running a publically accessible webserver on port 80 then you need to allow traffic through to port 80 (either directly or published via a proxy server). If your webserver or web served applications have vulnerabilities then the firewall provides zero protection. Firewalls are not magic shields. To a large extent firewalls are superfluous. You can provide pretty much the same protection at the host level by hardening the OS and turning off unnecessary services. However when you have a large number of systems it is much easier to control this at a firewall rather than on every single host.

Unfortunately some businesses seem to think that the firewall really is a magic shield and that they are therefore protected just by having one in place. Hence they become lax on application and OS level security and put off patching etc

While a firewall is not a magic bullet, it is a big help. For one, it cuts down on all the extraneous traffic. Even if you don't have a web server running your network is probably constantly being scanned for open port 80's. And the same for other well known ports. You may not run Windows at all but you can bet people are looking for it. And let's not forget port 25!!

And then, if you have an IDS in conjunction with your firewall it can be very good at detecting the difference between real users and attacks and can instruct your firewall accordingly.

Yes. Note I said

"

To a large extent firewalls are superfluous. You can provide pretty much the same protection at the host level by hardening the OS and turning off unnecessary services

"

I didn't say totally superfluous. :)

Firewalls have their place in securing a network but they are just one layer in

Re: Question for the Group

the security onion.

"Security is an onion because of the layers , not because you should cry while dissecting it ..."

However Michael Kraemers

"

OTOH, "security" these days means to organize your IT so that it has minimum cross section to the evil internet, rather than the choice of a particular OS.

Raise a firewall, hide business critical systems and important databases etc.

"

certainly seemed to be getting close to the firewall as magic shield fallacy.

David Webb
Security team leader
CCSS
Middlesex University

bill

--

Bill Gunshannon | de-moc-ra-cy (di mok' ra see) n. Three wolves
bill@xxxxxxxxxxxxxxxxx | and a sheep voting on what's for dinner.
University of Scranton |
Scranton, Pennsylvania | #include <std.disclaimer.h>

.