

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2007-07/msg00769.html>

- *From:* bill@xxxxxxxxxxx (Bill Gunshannon)
 - *Date:* 9 Jul 2007 18:51:30 GMT
-

In article <FA60F2C4B72A584DBFC6091F6A2B86840250A705@xx>, "Main, Kerry" <Kerry.Main@xxxxxx> writes:

-----Original Message-----
From: bill@xxxxxxxxxxx [<mailto:bill@xxxxxxxxxxx>]
On Behalf Of Bill Gunshannon
Sent: July 9, 2007 11:31 AM
To: Info-VAX@xxxxxxxxxxxxxxxx
Subject: Re: Is VMS losing the Financial Sector, also?
=20

[snip..]

You also need IE, Firefox or some other browser

on the

server to use these admin packages locally. The same is true for

other

platforms as well.

=20

Same rules. Just because you have IE doesn't mean you should be surfing

the web from the server. if you don't connect to untrusted machines you

don't have to worry about infection. They're servers for god's sake. if

you want to google soemthing go back to your desk.

=20

Point is that just by the fact that these services are on the server and being used means that all IE and IIS related security patches need to be

Re: Is VMS losing the Financial Sector, also?

applied. (and these 2 puppies are likely the most hacked and patched programs on the planet).

No, they don't. If they never have access to or from untrusted networks they do not. I suggested using only localhost or a private network but, as usual, you just changed the rules and said they can't do that. It's all about risk and its mitigation. If you insist that you must run in an unsecure environment then no OS is going to be safe.

In addition, many SAN Mgmt appliances that control your entire

SAN with

all your data are simply web based Windows or Linux servers. Some

do not

even have a command line option. Its all locked down and done

with a GUI

(appliance approach).

=20

Same thing. Just because they have to run a web server doesn't mean

you have to let anyone from outside the box access it. If an outsider

can't see the web server they can't attack it.

=20

It also makes it difficult to manage remotely and for it to send alerts remotely (page, email etc) when something happens. Remote management is no longer a nice to have – it is critical.

See, new set of rules. Remote can still be done from your private network using VPN so that even when you are remote you are connected to the secure network (thru appropriate firewalls and safeguards). Or, you can just have install your own dialups. I still run them here at the University. No one has used them in ages, but we aren't getting rid of them, "just in case"!!

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

[As some companies found out during SARS incidents in Toronto. Nothing like occupants of an entire building being told to stay home for 10 days to wake folks up on this critical item. Especially when a DC is in that building and no one can go near it for 10 days. I would think this an even bigger concern for the defence dept.]

There are ways around this that still don't expose your servers admin access to the outside world (and outside here means not just the INTERNET but also company LANS).

So, if there is an IIS or IE hole, then you absolutely do need to consider these a potential server issue – even on your appliance

boxes

out there.

=20

Not if access is restricted to "localhost". Might not be convenient for the sys admin, but you have to decide between convenience and safety.

In the Army we call that Risk Management and it can be applied to just

about everything. Identify the Risk. Reduce the Risk. Live with what's

left. If outside access is absolutely, positively necessary, put it on

a lan that is not connected to anything but the sys admin's computers.

Additional NIC;'s are cheap and VLAN's can do wonders for isolating

traffic. Or, if the risk is considered great enough a second totally

disconnected network but that's probably overkill.

=20

Bill – we are talking about DC's with hundreds and in some cases thousands of Wintel servers across the company. We are not talking about a few servers in the local server room.

VLANS have some benefits, but they also raise the requirement for all

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

servers to add NIC's, switch port counts need to be increased, and the complexity of TCPIP mgmt increases significantly as well.

Its all about risks. You have to decide how much of a risk it is and take appropriate action. Cost is often a balancing figure in risk assessment. But saying it can't be done is just ridiculous. What you are now trying to say is not, "It can't be done." but rather "It is too expensive." How much is risk mitigation worth?

You asked how a server can get exposed to a virus ..

Laptops, PDA's, memory sticks, cell phones etc are constantly

traversing

from external networks (airports, hotels, home) to internal

networks

bypassing the firewalls.

=20

Don't allow them on your network. Period. I have a personal laptop.

I can take it to my office at DISA. I can not connect it to the network.

I was talking about business laptops that are locked down. Of course, personal laptops should not enter company property.

The ones that company Sales, Marketing and Exec's all use today. I use a company provided laptop with a personal firewall product + latest in AV software which runs every night (I am paranoid about sending a Cust a doc with some buggie loaded).

I run AdAware all the time. All it ever finds are data mining cookies. I could fix that by turning of cookies, but then there are sites I could not use. I could fix it by not visiting these sites. :-> There are lots of ways to eliminate this threat too. But I have decided that the risk is low and having AdAware throw them all away every day is acceptable mitigation. I travel with my personal laptop all the time. I have never had a virus, trojan or any other kind of malware hit it. This is done by a combination of things, all of which are part of good admin. The

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

machine is somewhat locked down (I do have the admin password, most normal users would not.) I run an anti-virus and FireWall package I trust. And I am very careful about what sites I visit. (When someone sends me an email saying something like, "Wow, check out this cool website." even if it is from someone I know or even a relative, I usually just delete it. I never visit the site. (There are no "cool" sites on the web!!) I have decided this is acceptable risk mitigation. Of course I always have the option to just never connect to the INTERNET. :-)

This business laptop of mine gets used remotely (airports, hotels, conferences, home) and in the local office. This is exactly the model that likely 75% of most companies follow today.

If I run AD-Aware or Spybot, I know it will almost always find "buggie" stuff that the FW and AV package missed or did not clean-out. While I am assuming these are just marketing buggies, I really have no idea if that is the case or not.

So, you are obviously not that experienced or you would know what all of this is. That's part of the job. I am the guy others come to when they have a problem. "I don't have a clue." is not an acceptable answer.

The point is that laptops today are extremely hard to totally lock down without disabling the power on button.

Sorry, I don't agree and I have seen enough examples both inside and outside of .mil to support my opinion. You are free to spend your life believing otherwise. Until we have VMS laptops what we have today is the facts of life.

Memory sticks? When I worked on the network in Germany they were locked out at the top of the forest. You could stick it in the USB port but it wouldn't do anything. Same thing for all those other devices. If you consider them a threat you don't allow them to connect to your network. My brother works for an insurance company. He has a company laptop. He does not have any admin rights. He can't install anything,

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

deliberately
or by accident. It is locked down pretty much as tight as the DA
systems
I work with (much to their credit!!) Having them locked down this
tight
does not prevent him from using it to do his job. Of course, all
access
to the network is via VPN thru the company. No random network
access, no
untrusted access, no hacking. He has never had an incident
involving
this system. It can be done.
=20
=20

The trojans, worms, viruses etc these

personal

devices might pick up on external networks are typically
designed

to

propagate themselves and /or look for servers with known
holes

and

exploit them.

=20

Not if you don't allow them to connect in the first place. One has
to
understand the difference between business and personal. "And
never
the twain shall meet!!"

See above note about locking down business laptops. To do this properly,
most Sales and Exec types would object to a central group disabling the
power on button as it might tend to limit the laptops use.

I never suggested disabling the power button, that's your idea. But not
letting people put un-trusted devices on their computer is no different
than not letting them put un-trusted computers on the company LAN. It
worked fine over in Germany. People bitched, but then they bitched that
the coffee wasn't very good either. Strangely, not letting them stuff
thumb-drives in everything didn't stop people from getting the job done.
They just had to use the network to move things from one laptop to another

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

instead of modified sneaker-net. This proves much more secure for the data concerned as it prevents "leakage" as well as infection of the computer. In this day and age of Isot hard-drives full of customer data or SSAN's I would think that businesses would be looking at things like "leakage" as much as DOD does.

=20

If you were a bad type person, what better approach to get into a

large

corp like a stock exchange than to write a trojan, worm etc that

gets on

an employees personal device (laptop or ? that all have browsers

and

sometimes IIS services running themselves) installed directly on

the

Cust internal network and then looks for known server holes?=3D20

=20

Read my lips. No personal devices on the company lan. Period.

And

that's just physical security, we aren't even talking MS here. You don't let strangers wander in and out of your computer room, do you?

So why would you let untrusted "strangers" connect to your LAN?

=20

Course, you could always take away the employees (traders?)

Laptops and

PDA's ... yeah right.

Re: Is VMS losing the Financial Sector, also?

=20

Not take them away. If they need one fro business you provide it and you see to it that it is suitably locked down. And you don't allow personal PDA's and laptops on your LAN. Period.

=20

See above.

Try telling Sales and Exec's that they can not use their company provided PDA's at work. That will surely bring a round of laughter.

I said personal. If they have a company PDA it should be locked down just as tight as their PC. And, being as with the impending demise of Windows CE :-) I don't think there are many PDA's still running much Windows. Mine doesn't. The last one I had that did was my Compaq Aero.

Ever wonder why the nick name for blackberry is "crackberry"?

Risks!! If it can't be trusted, don't allow its use. If you must allow its usei knowing that you can't trust it, don't argue that you can't secure your network. And don't blame the device. You chose to use it.

Now see above notes about whether a server platform that has 5-20

new

security patches released *each and every month* seems like such

a good

future platform strategy for important applications.

=20

Works for me. The only "virus" on our network during my trip to germany was on paper only and required us to go through all the procedures we would have done in the event of a real virus. This was to test our

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

knowledge of and ability to perform all the necessary technical and paperwork requirements in the event of a real one. A real one never

happened. Probably because even though all of these machines coming

from all over the world were known to come from other secure networks

they had to go through a "decontamination station" prior to going

on our network.

=20

It takes a good and well defined strategy involving physical security,

administrative control and technical competence but any system can be

secured. The biggest problem is walking that fine line between security

and convenience to the user. But it definitely can be done. I

know,

because I have to do it.

=20

bill

=20

If you have company provided laptops that get used on external networks, then I can almost guarantee that these laptops have "buggies".

And I can assure you mine doesn't. Kind of shoots down your theory.

Like I said, the worst thing found is "tracking cookies" and I can stop even that if I really want to and am willing to accept that there are sites I will not be able to visit. But they are not a threat so

I accept them. I imagine a number of them are from .mil sites anyway as many of them require that cookies be turned on.

I am not saying the steps you are promoting should not be done, but rather that doing these alone in the hope that you will not have to apply all these known monthly server security patches is not a sound strategy.

OK, believe what you will. I have worked in many environments and seen lots of secure Windows systems, both servers and desktops. It can be done. It takes a lot to do it. Starting with physical security, mandatory personnel use procedures and very serious sys admining. But it can be done. Many here will never accept that and they are free to loose sleep every night thinking the world is hacking into their PC's. I sleep well at night. Especially since applying much of what I have

Re: Is VMS losing the Financial Sector, also?

Re: Is VMS losing the Financial Sector, also?

learned maintaining .mil PC's on my University stuff. And I am not done yet. I will be making some major changes to everything here from the network on up. We will be even tighter when the students get back this fall. And in all likelihood, they will not even notice it at the user level, except for the fact that they never sit down to an infected workstation!!

The sophistication of the bag guys and their "buggies" today + the volume of monthly security patches for Windows/Linux is just way to much of a risk to depend on.

You keep harping on this one item even when it is shown that there are ways around it. Nothing is going to convince oyu otherwise. Too bad, really. Risk is a bad thing. It leads to all kinds of stress. But it can be effectively mitigated. But first, you have to admit it's possible.

bill

—

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

.