

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/msg00756.html>

---

- *From:* "Main, Kerry" <Kerry.Main@xxxxxx>
  - *Date:* Mon, 9 Jul 2007 12:20:23 -0400
- 

-----Original Message-----

From: bill@xxxxxxxxxxxxxxxxxxxxx [mailto:bill@xxxxxxxxxxxxxxxxxxxxxxxxx]

On Behalf Of Bill Gunshannon

Sent: July 9, 2007 11:31 AM

To: Info-VAX@xxxxxxxxxxxxx

Subject: Re: Is VMS losing the Financial Sector, also?

[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.

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.

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

RE: Is VMS losing the Financial Sector, also?

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).

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.

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.

[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.]

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.

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

RE: Is VMS losing the Financial Sector, also?

RE: Is VMS losing the Financial Sector, also?

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  
issolating  
traffic. Or, if the risk is considered great enough a second  
totally  
disconnected network but thats probably overkill.

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

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.

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).

This business laptop of mine gets used remotely (airports, hotels,

RE: Is VMS losing the Financial Sector, also?

RE: Is VMS losing the Financial Sector, also?

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.

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

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, 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.

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.

RE: Is VMS losing the Financial Sector, also?

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.

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?=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?

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

Laptops and

PDA's ... yeah right.

RE: Is VMS losing the Financial Sector, also?

RE: Is VMS losing the Financial Sector, also?

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.

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.

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

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.

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 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 theya ll had to go through a "decontamination station" prior to going on our network.

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

RE: Is VMS losing the Financial Sector, also?

RE: Is VMS losing the Financial Sector, also?

know,  
because I have to do it.

bill

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

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.

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.

Regards

Kerry Main  
Senior Consultant  
HP Services Canada  
Voice: 613-592-4660  
Fax: 613-591-4477  
kerryDOTmainAThpDOTcom  
(remove the DOT's and AT)

OpenVMS – the secure, multi-site OS that just works.

.