



RUNAS RADIO



<http://www.runasradio.com>



Richard
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg
Hughes

Text Transcript of Show #0975
(Transcription services provided by [PWOP Productions](#))



Dana Epp Secures Our Virtual Machines!
February 18, 2009



[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #97, with guest Dana Epp, recorded Thursday, January 29, 2009. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com. You can follow the boys on Twitter at twitter.com/runasradio.

Richard Campbell: This is Richard Campbell and you're listening to RunAs Radio. With me as always my co-host, Greg Hughes.

Greg Hughes: Hey, how is it going?

Richard Campbell: Good. We seem to be on a roll of security shows lately.

Greg Hughes: Yeah, that's okay.

Richard Campbell: You're not complaining. Yeah, it's your stuff, right?

Greg Hughes: Yeah, yeah. That's really what we should be doing, isn't it?

Richard Campbell: There's lots of stuff to talk about.

Greg Hughes: We can't have too much security.

Richard Campbell: Well yeah, you can. There's a point in which there is no doors into the room.

Greg Hughes: Good point. Yes, security is a way of doing business as opposed to should be a way of doing business and facilitating it as opposed to a way of shutting it down and making it impossible.

Richard Campbell: Right. That's what all you security guys say.

Greg Hughes: That was my short soapbox right there. But yeah, you're right, we had a good opportunity to talk about a number of different security threads and to talk to someone. We'll get to do that a little bit more today.

Richard Campbell: Yeah, and I'll get some love in the next few shows, and by all means if you don't like security shows you can send us an email and let us know, or if there are other topics you want to hear from, info@runasradio.com.

Greg Hughes: Yup.

Richard Campbell: All right, let's jump to our guest that is Dana Epp. Let me see his bio here. Dana Epp researches software security and sets the corporate vision in the convergence of information security principles and practices with digital information asset protection, Scorpion Software -- holy cow, OK he's a security geek.

Greg Hughes: Blah, blah, blah.

Richard Campbell: Dana.

Greg Hughes: How is it going, Dana?

Richard Campbell: I can tease my friend, we're from the same part of the world. We saw each other just last week at Tech Days.

Dana Epp: Great. Where I was doing presentations on security.

Richard Campbell: You were doing stuff on security, and I was talking about Vista Bridge of all things but nobody seems to know anything about it. I think it's the only way to actually make your apps look like the Vista apps. Of course now you have to wonder if that's actually a good idea.

Greg Hughes: Without actually making them Vista apps, yeah. So Dana, what were you talking about the other week?

Dana Epp: Well, I was talking about how to secure your virtual environment so when people want to start utilizing Hyper-V in a deployment scenario, how do you use things like AzMan and a whole method of using authorization manager and bridging all that stuff together to provide a finer grain role control for that. When people need access to different VMs, they can get that without...

Greg Hughes: Cool. So you mean it's not like just automatically secure out of the box all by itself?

Dana Epp: Hyper-V has got a lot of ways of managing it if you're like a single role environment where one person is dealing with it. The issue comes down when you want to have multiple people. Let's say you're a SQL database administrator and you want to have the ability to reboot your SQL box and you need to do that at the console level because maybe something got wrong. Well, under normal scenario, you have controls on the physical box so you can do that. What do you do in a virtual environment though? Normally, that gives that person complete administrator credential which means they have access to every single virtual machine on the Hyper-V server which is a big risk and so you can use things like authorization manager and



restrict it down so that SQL manager only manages the SQL VM and that's something that a lot of people don't know exist in Hyper-V which gives it really nice security principles to apply like it can match up with it.

Richard Campbell: Now, the way I hear you describe this, Dana, it sounds like we're talking about security specific to doing stuff with VMs. Don't the normal security roles like in Exchange and in IIS, are they just the same in a virtual machine?

Dana Epp: Well, in many cases they are because when you treat what's going on in the operating system inside the child, yes, you're going to still file the same security principles and practices to how you would walk down Exchange. The issues that come into play though when working in a virtualized environment is that there are lots of other considerations that need to be accounted for like how do you deal with a file that can be just copied down to a USB drive and walk away. Normally you don't worry about an Exchange Server being picked up with some big box in a server room, but if you have the ability of simply copying a VHD file off of the Hyper-V server and then walking away, that's a different kind of risk you need to account for. Other things include things like if you're using systems in a virtual machine manager, any kind of VM management tool where you going to have VHDs that you might need for roll back or apply your other concerns like are you making sure that when it comes back up into the environment that it's up to date, are all the patches applied, or are all the security paradigms that you would apply to that server matching whatever your corporate security policy is, and it's kind of a risk if you have because sometimes you might have dormant VHDs, you know, like let's see you bring up a brand new Windows Server 2008 box, you have a goal to play VHD there that you're going to bring up and clone. As soon as you bring it up on the internet or on the network that is connected to the internet, they're exposed to any risks because it is not patched yet, whereas, in a normal brand new install, it's the first thing that happen, the security policy set it up so that no one can touch the server until all the updates are applied. These kind of little nuances just to consider whenever you try to bring this stuff up? Yes, hardening the OS, hardening the application, everything still exist but then there are other considerations that needs to be applied when you consider what you're trying...

Richard Campbell: Didn't I recently read that Microsoft made a tool where it's possible to patch a VM without sort of fully starting it up?

Dana Epp: Sort of. What they've got is they got an ability so that it will bring up a VM, apply the patches, and then bring it back down.

Richard Campbell: Okay.

Dana Epp: And at the time that it comes up though, it's going to be connected to a network. Depending on how it's configured, it will have the ability to be on that network. Now, what's nice is in SDMM, because that's behind the scene, everything like SDMM is driven to PowerShell and so they've got this release with PowerShell script, they can let you do things like when you bring this kind of stuff up in the VM you can reconfigure it, you can reset it so you could theoretically put it on a quarantine network that's maybe isolated with the management gateway and it's got WSAS behind there and then you can apply the patches and then bring it back down and it won't touch it, and that's a good way of doing it. I'm more interested though that there is some research going on right now where they're looking to do that offline so that it doesn't have to bring it up, because again to the day, the VHD isn't a manageable file that you could theoretically amount to read only and apply it. There's some other things that make that much more difficult like just some of the policies saying you need to apply to make that work, but I'm actually looking forward to have that day because that means stale VHDs that might be two years old like you're going to bring up as a base can always be up to date and patched...

Richard Campbell: Yeah, I'm just thinking about the battle there of maybe I've got a VM here that normally is part of a web form and I spin up new additional ones as I need more performance and so I don't want that coming up to be patched and actually try to join the pool when it does it. So I guess there'd be some tricks around how do I configure this so that I can bring it up, get the patches in and bring it back down without ever trying to do any of the things it was actually built to do.

Dana Epp: Right and that's one of those things that they've got with this -- I can't remember the actual name of what that tool is but it just came out a couple of months ago. It's on TechNet for download. It gives you the ability to do that, basically roll it up, and as long as you put it up in an isolated state nothing prevents you from putting it on a special NIC that is not internet phasing. The trick is making sure it still gets the patches you need to apply, so depending on how you use the tool you might apply it directly or a better way is to have something like the ISA Server that's up to date, that's isolated and quarantined in that valid environment so you can accomplish what you need to and it's nice because you can actually see some very interesting things like applying -- what I would do in those kind of experience, is one of the reasons I would like these things like Windows Search 2008 and pretty much every VM that you do know, it's that we can apply Net policies so we can actually have the system automatically quarantined



itself because the Net client policy will say, well, you're not patched, I'm isolating you until you do it. So there's some other Microsoft technology that you can apply at the same time. Unfortunately, that doesn't exist or it's extremely difficult to configure in things like Windows Server 2003 so there's a plug-in wire people should be using in all other VMs.

Richard Campbell: Are you seeing the adaption of Hyper-V going quickly? I still see, of course I'm working with Microsoft a lot, a lot of their sample stuff is coming out as Virtual Machine rather than Hyper-V.

Dana Epp: I think part of that is just branding and recognition. At the end of the day, VHDs are VHDs other than some internal components that you need to install, and the others, still virtual server and more importantly a lot of those testing of Microsoft release in things like Virtual PCs which are not Hyper-V. The reality is we take a look at production server, what are we going to use in an IT Pro environment for rolling out production VMs, and what's interesting is that there's a lot of different statistics that have been put out there from lots of different study groups like the one that I think is pretty cool is the IDC that the white paper had said that the number of virtual servers are going to rise from about 1.7 million right now to about 7.9 million by 2010 and that's going to jump to about 14.6 dependable servers. If you think about that in that number with that same effect, for me physical servers that are out there, they're expecting to have four virtual servers, are always like virtual machines and it doesn't matter what we're using to do that, if that's Hyper-V or Virtual Server or if that's VMware or USX or standards, at the end of the day whatever that platform is going to be we have a lot of virtualized machines that can be out here by 2010. So Hyper-V, Microsoft has rolled out a very good technology that makes a lot of sense and so I think the biggest issue is that you need to have Windows Server 2008 and standard option curve for some ITP folks, there hasn't been there yet, it's coming but you need Windows Server 2008 to use Hyper-V and not everybody has done that yet. So that's a little bit of that, I think where the issue is that Microsoft is trying to battle.

Greg Hughes: So I go to, Dana, apps that are really cool and awesome session or class on virtualization and security. What are the key concepts that you're trying to get across? I mean, what are the things that people really, really need to know?

Dana Epp: Well, I think one of the key things is to understand where Hyper-V fits in the big role of things because there are some security goals that Microsoft had to put down when they were designing Hyper-V which makes it entirely different with a lot of other virtualization platforms that exist. It's like some of the things that they did was that they

made sure that they were providing strong isolation between the partitions. So like they cannot park unless you do what I would consider a standard IT means, like if you need to communicate the RPC you're going to do that in the network layer, you're not going to have the ability to communicate directly from between VMs which some of the platforms do allow you. Actually, there are some of the open source platforms that actually gives you the power that as you're spinning up a VM you can directly manipulate this stuff inside it. Microsoft said no way, it would not do that in a production environment because that reaches that isolation and it often then allows you to guarantee the confidentiality and integrity of the data. You can't touch it unless, you know, it needs the standard operating system mechanisms for authorization and authentication and all the other pieces in there and because it's all separated, they have such a small hypervisor. The actual hypervisor that runs this whole core thing is like about 350k, whereas if you look at something like ESX they are I think like 32 megabytes, and the reason is they got all these drivers and all these other stuff that's in there and that's from a security standpoint. When we think of things like patch management and driver management in that there is not this really interesting isolation between the parent and children partition and that's been something that's been very, very critical I think because people didn't realize that Hyper-V was designed that way which it does makes it much safer. The other parts of it though that I think is more critical is people trying to understand how to secure the parent partition, that's the most critical thing when we talk about Hyper-V, and my session at Tech Day is specifically on how do you secure that parent because there are some critical pieces that you can do which are needed from everything from how you install Hyper-V. A lot of people don't know that Windows Server core was designed in a way so that you can deploy Hyper-V and significantly reduce the attack surface of the base partition like the parent partition.

Greg Hughes: Sure, right.

Dana Epp: Because you're actually removing all of those binaries that don't need to be used and why that's important is if you take a look at, let's say, Microsoft virtual server that runs on Windows Server 2003, every update to Windows Server 2003 meant that you would have to bring down the entire box because you have to bring every VM down and the host and reboot. Well, okay, that's going to happen even in Windows Server 2008, but if you're running core, the actual patch of it is significantly reduced because there simply is no binaries there so you go from base install of 3 to 6 gigabytes down to one gigabyte and the main core reason is that all the applications are gone, there is no UI, there is nothing to update and that makes it much



safer because: A) From a productivity point of view, you're not bringing the box down all the time, and B) is that if there was a vulnerability that is found in that base system it is much more difficult to exploit if there is literally nothing running on there.

Greg Hughes: Sure.

Dana Epp: And that is one of the things I'm actually kind of scared of. I see people running, it doesn't matter what personal edition of platform that you're using, they're parent partition, they're installing stuff, they're like making it their domain controller. I'm just screaming at them going what are you doing, you don't run role and services other than virtualized stack in that parent because you need to isolate it and make it basically do nothing but the virtualizations.

Richard Campbell: Now that being said, you do need one physical AD server at least somewhere in your network.

Dana Epp: Basically, you can. There's nothing that said you cannot virtualized your active directory infrastructure. I would just highly recommend that you have at least one physical read only domain controller as a secondary in case the virtualized one has a fault or failure.

Richard Campbell: Right.

Greg Hughes: Sure.

Dana Epp: Because, you know, at the end of the day, like I looked at our organization, we're a pretty small organization so we're running small business server and what we've done is we've got Small Business Server 2008 running in a virtualized environment and then we have a small really, really old box that's a read only domain controller in Windows core as a failover so if the SBS 3M doesn't come, we still can at least log in and get access to stuff and fix it if we needed to.

Richard Campbell: Well, I'm just thinking about that host machine you need to come up in the domain. There needs to be a domain controller somewhere.

Dana Epp: Well, it's in a cache mode, right. So you can still even if the DC is not quite up yet. One of the tricks you can do is you could easily configure the VMs so that in order presence and how that all comes up, the parent itself it doesn't matter because it can wait for the DC to come up. You just kind of make sure all the other VMs and everything else don't start, there's an order of precedence and a timing that can basically delay the start so that the PC can get up and running, and in the case of something goes wrong, if you have that read only domain

controller as a physical box somewhere at least you have that as a backup and the nice thing is that like I said you can run that on Windows Server 2008 core with all -- like I think ours is an old 512 meg, actually an old desktop luxury and we just have it as a back-up domain controller just in case.

Greg Hughes: I think your point, Dana, correct me if I'm wrong, was that if people are building a virtualization machine and they're building that parent or that host machine, depending on your terminology, that they're also installing other services on there like domain controller services or active directory services or what have you.

Dana Epp: Yeah and we shouldn't be doing that because on that parent, there should be nothing installed on there, the only thing should be the Hyper-V roll, that's the only component on there, and then maybe possibly, if you're using something like SCVMM there's going to be some agents that needs to be installed in the parent host so that stuff really should be installed, but other than that I wouldn't recommend that anything be installed in this parent.

Richard Campbell: I'm actually poking around on this whole offline VM patching and it looks like the tool is called Offline Virtual Machine Servicing Tool.

Dana Epp: A very unique name.

Richard Campbell: Ah yeah, Microsoft has a knack for really bad names.

Dana Epp: Yeah. That was a cool codename, you know, but then all of a sudden they go away and got the stuffy business names but again it's their business and it has worked well for them.

Greg Hughes: The acronym you can't pronounce.

Dana Epp: Yeah. Well, there you go. Or you have 50 different acronyms that all mean different things but they're all the same thing.

Greg Hughes: So what else is important to be thinking about? You know, as the IT person who is security conscious in the case of what we are talking about and we are doing virtualization for the first time, and maybe a more abstract question or a step back a little bit question is I want to be able to do security better and I want to be able to virtualize and streamline in that regard, so how do I make those two things work for each other?

Dana Epp: Okay. Well, there are a couple of things that really help. Hyper-V actually have what I would consider a golden gem that very few people know about and that's the ability to apply it through as



manager or the authorization manager, an ability to apply different roles and operations to different people. One of the risks that you have when you talk about Hyper-V is that now you have what is called the role administrator which is pretty much the guy that has, oh God, like powers on that parent and that means that they have the ability of managing and manipulating all the children so what ends up happening is they can start and stop and modify and basically change how the behavior of any VM works. Any of the children can be controlled by that administrator and that's not always a good thing. So there are things like authorization manager. What this gives you the ability of doing is to apply this in like 32 different operations that you can apply through AzMan or Hyper-V. Things like can you start a VM, can you stop a VM, gives the ability of looking at the network property, gives the ability to change the network property. One of the really cool things that I like about Hyper-V is that in a networking side of things, you can create isolated networks like you can have complete DMZs all thrown out from different NICs or even virtual NICs to the virtual switch and what end up happening is that you can control who has access to look at that stuff and to modify that stuff. So now all of a sudden, we can have different types of administrators having different access to the VM directly so we could have it. So in our own organization here, my developers, they have to have access. We have a box called QADS which is a Hyper-V box and what we've done is apply different AzMan roles to create these different roles and then we give them to the developers so developers can manipulate these VMs but they can't touch the actually automated testing VMs because it would really be bad if they screw up our daily automated testing framework and we can do that by just applying those AzMan operations for those roles to a group called developers and that applies in a way and restricts it so that they can do only certain things. Meanwhile, me as an administrator, I have full access and I can determine who needs access to what so they can do that and then you top that off with Hyper-V manager which is the tool you use to manipulate and manage and this can be run from desktops. So what's nice is you can run the Hyper-V manager on our Vista machines and we can literally just start and connect that to the Hyper-V server and base on what permission we have we can only access and manipulate from console or by RDP, however, we've got it configured and that's really nice. What's sad is that not a lot of people know that it even exist from a Hyper-V point of view. You can isolate it and control however you see fit.

Richard Campbell: You're definitely delineated to distinct work cases there. When using VMs for development and testing is one thing, when you're using VMs in a data center environment, I guess the two big roles I can see and that you want to secure

independently would be the ability to spin up new VMs or relocate VMs versus actually modifying or creating them.

Dana Epp: Yeah and you can do that because it's one of the things that you want to see. What's interesting is that where AzMan is applied directly in Hyper-V server, you can go one step further. If you go and purchase Microsoft System Center Virtual Machine Manager, they also have the ability of having AzMan and even have a self-provisioning portal that's web-based that is using the same AzMan operations and role so you can actually control how people not only spin it up only once and like you said they can target them onto different CPUs so you can have what they call quick migration so you can say, okay, so one of the things that I talk about, like I said at Tech Days, was talking about how you can physically separate a VM in what I call domain of trust and what that really is, is that if you got let's say a physical server who is a production server that's internet phasing in a DNZ let's say, that's going to have different security policies applied to it than a QA box in an isolated LAN, but what's interesting is through things like SCVMM you can retarget in and say okay, so I'm running on this VM, we're testing with it, we're happy with it, now we're ready to deploy it. You actually have the ability, depending on that permission set of what they've done and what they're allowed to do, you can all stand and say, okay, I want to now deploy that VM in the production server and what you're doing is crossing a boundary of trust when you feel or they feel, depending on the permission, that that should be done so that means I can do something as simple as let's say I got a new Exchange 2007 box that I've got somewhere and as part of that I have an isolated management system, I don't know, like in our case here we have some PowerShell stuff that's running on an old Windows Server 2008 box, I don't want that PowerShell, those scripts and everything that's running on there to be public phasing until we've audited it and when it's kind of audited I have the ability to say, okay, I'm not going to take it from this isolated network where we tested it, we made sure everything is good, I'm now going to roll it into production. Now, how do I roll it into production? I literally kind of just do a quick migration from Target A host and bring it over to Target B host which is on a different trust boundary at a different network and one nice thing is I can apply that and I can apply it directly on that server through the AzMan world, but more importantly I can directly address SCVMM base software permission...

Richard Campbell: Obviously, some smart people have really thought through this problem.

Dana Epp: Well, you know what's funny? It's that this is like a personal gripe I have. As a Microsoft enterprise studio MVP, there's lots of



security technology that's under the hood in the operation system.

Richard Campbell: Right.

Dana Epp: That just aren't being leveraged. People don't realize this but AzMan actually existed in Windows Server 2003 forever and application vendors have had the ability to apply and use the AzMan system. They're giving it free on stores so if they want to create their own isolated authorization controls for their application, they could do so, or they can leverage existing authorization controls that are in there and why that's important is that we're coming into a world now where authentication authorization are separated out, but more importantly the applications needs to be able to work on their own and not care about how people are being authorized or authenticated and if they can start applying this whole aspect of using things like AzMan and using roll-based security, it means that when they apply this on someone who has a certain role they might get access to all these different tools. These applications then will apply this logic for things like AzMan in their own apps. We would actually see a lot of benefits from that. I mean, if we provision someone else to do a role of the accounting department and we know what's all in there. Yeah, we can apply certain things like security groups and so forth in AP but at the end of the day the applications themselves, because they're not aware of what those roles are, I'm not specifically right so that's not going to work, but if you use something like AzMan and you use role-based security, your texts are applying all these other types of technology that exist out there like you can apply things like the Geneva framework, you could use active directory federation services, you could apply AD domains across ports because you could use a centralized AzMan roles in the stores and it can get really complicated or it could be very, very simple, you could have it all centralized in one way and create these claim-based applications that could use these roles to do it all. Unfortunately, Microsoft sees it in some department which is what we're seeing in Hyper-V but there are lots of other departments where they're not and I've always been frustrated because I think things like SharePoint should have leveraged that. If you had those proper AzMan roles, that means that the same roles you might apply to controls in Hyper-V might be what you'd use for publishing in certain areas in SharePoint. Now, who said we couldn't actually have configuration?

Richard Campbell: You started off this point that this particular rant saying I wish other software developers would do this, but starting to Microsoft that's actually doing this consistently across their product lines.

Dana Epp: That's right and you know, it's funny, it's everybody. So here's the biggest thing that I think drives me nuts just as a developer, it's that, and I see this too and I'm not saying that we're perfect because you know although we build claims with applications sincerely, the reality is we could probably do it better if we can leverage the same ecosystem and systems that other people are using, but the reality is this, it's that whenever you design systems in software, you need to leverage whatever the operating system has to your advantage for security. So we see from vulnerable software applications that simply don't use things like proper ACL, they're not locking down stuff even though Microsoft has a great way of locking down file access down. We see things like the whole reason UAC was born was because people, well, quite frankly, developers were lazy and they would just say, oh, I'm just going to write directly to the registry in ways I shouldn't do because I can, and UAC all of a sudden put it in our fate as developers, hello, you're writing some place that is considered privilege and you shouldn't be allowed to do that.

Richard Campbell: After how many years of being told only write to the user's portion of the registry, not the machine portion of the registry, don't write to System 32, don't write directly to program files, now we're finally enforcing all that.

Dana Epp: That's right. You know, let's look at it from an IT perspective. How many times do we see IT administrators installing applications and then putting the document folders or basically what is going to be considered the user data in the same freaking program file directory and what do they do, they just go and change the app where they full read and write in full and that drives me nuts when they do that, and you know, when designing security either from our design applications from developers side or even from an IT Pro side, we got to use the infrastructure that's there and the reason is that, 1) it's audited way better than some of the half-baked stuff that I see people do, and the second thing is that if you leverage operating system pieces, so everything, from using the right crypto library, I hear about guys having vulnerabilities in their applications so they wrote their own crypto library, it's like you realize Microsoft has audited and done all these already, why would you use somebody else's stuff, or we see people that are saying okay, I'm just going to write directly to program files because I own that folders so I have the rights to add privileges whatever I want. I just say okay, well, that's just you not caring or being too lazy to do it right and a lot of people think that UAC is a security mechanism, I don't, I think of UAC as a warning to allow people to realize they're running crappy software. That's one of my view.

Greg Hughes: That's a good point.



Dana Epp: And at the end of the day, we're actually seeing, at least on the MVP side, we're actually seeing a significant reduction in even things like UAC prompts because developers are starting to realize, hmm, maybe we need to write safer. You know, Microsoft brings out lots of tools from Visual Studio down to the installer tools to make it a little better and easier, they have an SDL process that's helping train people to do it better. As IT Pros, we also need to apply the same kind of logic so we need to be using ACLs properly, we need to be using things like AzMan, we need to be using active directory more efficiently and in Hyper-V at least they saw that and they've applied that knowledge into that and we just need to get more people using Hyper-V to know that that even exist.

Richard Campbell: I do think you're a bit of an idealist here. We're just trying to get pass everybody is an administrator to you're an administrator or you're just a regular user. You're not talking about granularity within the administrator set of rights. I think you're a dreamer, Dana!

Dana Epp: Why, you don't have to be a dreamer, let's give a perfect example here, because I know you do -- you know, you obviously do lots of interviews and talks with lots of developers, what's the first thing that developers does whenever he has got his own box? He requires that he has full administrative rights so that he can code.

Richard Campbell: Absolutely.

Dana Epp: Why is that? Because in Visual Studio, they need that administrative rights. That's a load of bull. I run as a standard user. I don't run as administrator. If I need that, I elevate to run as administrator and get an actual prompt and type in my administrative credential. Even if I was not an administrator, I can still get my work done and the reason is because 9 times out of 10 when you're doing development, you do not need administrative rights. In areas where you think you need administrative rights, that's just a posse change, you can just change it. Maybe you need enough permission to register COM interop if you're writing, let's say some components, you need to write to the registry, you could apply a control for that. Maybe you need to have some privileges to do certain things. Okay, well, do the system support that? In this case, we're talking Hyper-V here. If I need to spin up a VM, I just need that permission to spin up the VM. I don't need to have complete administrator rights. The problem is that we always think that security is a burden. We think of it as a position where it's going to burden me, I don't want it. I'm a developer or I'm a IT guy, I need full control, and that's not what should happen, least privilege which is what we're really

talking about here, giving just enough privilege to do your job. You will never see security, you'll never see things pop-up unless you do something you're not supposed to. If you start getting these blocks, that means that as the security administrators they haven't done their job to make that right or work or they haven't been screaming to the right people.

Greg Hughes: Sure.

Dana Epp: As an example, I for years have been yelling at Microsoft telling them that I think they've design Visual Studio wrong. I think they should be isolating out these tools to do things like registering things, bringing up the debugger that connects up to IIS, those should be done in smaller tools that can be isolated and elevated in their own rights and things like your freaking editor should not need administrator privileges so you can do things. That's just design feeling that they've got and I believe they're wrong but that's my opinion because I'm a security geek and quite frankly you're right, I'm an idealist. At the end of the day though, 9 times out of 10, when people say they need administrator rights, they don't. They're just thinking it's easier to get around if they don't have to do anything and that's just a wrong attitude and it has got to change.

Greg Hughes: Right. You could call it the laziness problem.

Dana Epp: It is but it's the reality. People want to get their job done. Computers are there to let them do their job and when they go and put something like a UAC prompt every time they try to, I don't know, do something like -- it's kind of funny, I was like talking to a guy recently who is complaining about Vista, he didn't like it because there's always UAC prompts. I said, okay, are you sure you're running Vista? And the funny thing was he only saw, he never actually run it. So I gave him a free copy because as an MVP I got buckets of dollars for buying Vista licenses and so I gave him a licensed Vista install permit. He comes back a month later and he is complaining to me and he is saying, you know what, okay, it's not as bad as I thought it was, it's actually pretty good but there's some really stupid things like why do I have to elevate to flush my DNS, and I said because that's a privileged operation. Yeah, but I still need to do that. I'm like, okay, let me ask you this, how many times do you flush your DNS? And then all of a sudden he's like, well, that's not the point. And I go, that is the point. You know, if you want to do privileged operation, yeah, you need to elevate, it's not hard, you just right click and bring up your command window and type IPCONFIG/dns update and it will work fine, but the reality is it's not an operation you're doing everyday. I haven't seen a UAC probably in two, three weeks and I think that's because I didn't install from...



Richard Campbell: Right.

Dana Epp: And the reality is it's designed right. I run it as a standard user, not as an administrator, I've got the right privileges to do the things I need to do and I never see this problem and that, I think, comes down to how IT administrators administer and apply security policy craft in network.

Greg Hughes: The old adage that there are no technology problems, there are really only people problems kind of applies here, that applies to...

Dana Epp: Yeah, that's very true.

Greg Hughes: That applies to people who are designing the technology or the people who are deploying it or the people who are using it. They're taking the short easy way out.

Dana Epp: Yeah and the thing is that the weakest link in security to human factor anyway, it doesn't matter how well you deploy it, there will always be somebody who is going to find some different ways that it's going to block them or get them around it and what you've got to do, the idea is that everyone is going to get a line and say, you know what, security is for the betterment of our company and for our users and for everything and so we need to use it to protect us but we also can happen to be a burden that's stopping us from getting our job done and I think administrators, let them do their job.

Greg Hughes: And I think if we just do security really well, then it enables us to do our jobs better.

Dana Epp: That's right and even the real look of things is if you do security well, no one will know because that's the whole idea. If you do it right, they're never be confronted with it unless they do something they're not supposed to do.

Greg Hughes: That's a whole different topic. You know, on the virtualization thing, before we let you go, there's one recurring question that I hear come up all the time and you sort of have this apocalypse of virtual machines where you have an organization where the great thing about virtualization is that it's easy to spin up a virtual machine and I can do it quickly, but the terrible thing about virtualization is that it's so easy to spin up virtual machines and I can do it so quickly you end up with virtual machines that are sitting around stagnant that somebody then goes and grabs, they're taking up tons and tons of storage space. Is there a really good actual workable solid answer to dealing with just the onslaught of VMs?

Dana Epp: Yeah. Well, actually the way I do it here is that we use proper network isolation with VM. So if someone brings up a VM that we have not authorized, it's isolated in a way that it's not going to be able to do much. We use net policies to pretty much anything that comes up on the network, we'll not be allowed to talk with our AD, we'll not be able to do anything, we'll be quarantined and isolated off in a place so that -- can I bring prevent someone from bringing up a VM? No, of course not. But can I prevent that VM from doing anything or communicating with our organization? Damned straight, I can. Now I can do that only with IP sect policy and do that through just standard networking. I've got VM controls, I've got physical switch control really to make sure that that's not going to pollute our network or worse yet go out and pollute other peoples networks. I'm liable...

Greg Hughes: Sure.

Dana Epp: I'm liable when, you know, let's say someone brings in a VM that infects this organization, I'm liable for that. If that thing goes outbound to the rest of the internet as a good medicine, I don't want to allow that and that's where things like management gateway can allow me to, you know, people need to be logged in before they can get out of a network and...

Richard Campbell: But this is the same as if a foreign laptop comes into the network.

Dana Epp: Exactly. If someone comes in and plugs in a laptop in your network, it gets isolated, there's nothing that they can do to get on that network to do anything. Is it perfect? No, there's always going to be something to get out there but there's lots of cool new technologies that exist and not just because it's cool, but because it was designed in a way that makes sense. Things like NAP -- it's a built-in role that you can apply directly on a Windows Server 2008 and just like cost you nothing.

Richard Campbell: There's a great security synergy between NAP and Hyper-V here that I don't think has been explored enough yet.

Dana Epp: No and so when we're talking about staying at VM like the funny thing is that what prevents someone from downloading the free virtual PC, installing it on their laptop as a user, they'd only need administrative rights for that side of it, I mean spinning up a VM inside there, well, there's nothing so they can bring up a little Linux box that they can automatically start hacking the network. In our case, what we do is that if a foreign IP that's not connected to the domain TMG, (Threat Management Gateway) is going to just say I don't know what to say, we will



keep that isolated over there until they have log-in and that gives us only some control.

Richard Campbell: Right.

Dana Epp: Now I have to say, you know, we're always talking of me being an idealist, the reality is that I only have to manage about, you know, 50 to 60 nodes in this network so it's very small in comparison to big networks like thousands and thousands of nodes in that, so yeah, I realize that. But on the flip side of it is outside of the technology we can apply, there are also human heuristics and more importantly human training. Quite frankly, anyone who brings up a VM in a network that's not on the QABS box which is our only, what we call, it's an isolated VM network basically and if we find out about it then we're going to have words, so that's an HR problem. It's an HR problem, that's not a technology problem.

[Laughter]

Richard Campbell: You don't want to make Dana angry.

Dana Epp: We try our best to defend against it by indicating that if someone does bring that up, we look up for it and I like to say like we have wireless here, it's isolated with its own subnet and you know the theory with this, I've seen employees bringing their own laptops to at lunch go play GuildWars or do whatever. Do whatever you want, just don't put that polluting on our network and within reason and we make sure that we teach them. If you're going to bring up stuff and do that stuff, you need to do that in a mature way and we have to watch it. That's human heuristic, that's an HR problem, not a technology problem.

Richard Campbell: Dana, always fun to talk to you, man.

Greg Hughes: Sure appreciate it.

Dana Epp: Hey, no problem. Thanks for having me on.

Richard Campbell: And we'll see you next time on RunAs Radio.