



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 #035
(Transcription services provided by [PWOP Productions](#))



Chris Avis fights Spam on Exchange Server 2007!
December 5, 2007



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

[Music]

Carl Franklin: From runasradio.com, you're listening to RunAs Radio, the weekly Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing show #35, with guest Chris Avis, recorded live at DevConnections, Thursday, November 8, 2007. RunAs Radio is produced each week by PWOP Productions, offering professional media and podcasting services online at pwop.com.

Richard Campbell: Hi there! This is Richard Campbell. You're listening to RunAs Radio and we're live at DevConnections. I guess this is really the Connections Conference because we're on the IT side of things here in Las Vegas and with me, as always, Greg Hughes.

Greg Hughes: Hi, everybody!

Richard Campbell: All right, guys. Well, let's get right to it. We have Chris Avis sitting beside us, amazingly. Chris, tell us a little bit about yourself and we're going to wander off in the land of spam today, which I'm really looking forward to, guys.

Chris Avis: Well, that's kind of unusual because most people don't look forward to spam but...

Richard Campbell: I don't look forward to spam. I need help, let me tell you.

Chris Avis: Okay, there you go. All right, so my name is Chris Avis. I'm with Microsoft. I'm an IT Pro Evangelist and I'm primarily charged with speaking to IT professionals about all of the cool products and technologies that Microsoft has to offer.

Greg Hughes: So you're part of a team of people that is... Really, your job is just to get the word out.

Chris Avis: Yes, yes. We are part of an engine. We have no quota, so we are not responsible for sales, but we'd like to try to tip people towards the technologies. The big part of it actually is marketing as well, raising the awareness of things, features, capabilities that software has that people just don't know exist.

Greg Hughes: I'm curious and I don't want to get off topic here, but I am curious. How do they measure your performance at Microsoft? If you don't have a quota and it is not the quality of software that you are building, how does that work at Microsoft?

Chris Avis: So, we are part of a feedback loop between marketing and the development team.

So we get information and transfer that back and forth. As a measure of performance; it is how many people we can reach and then of course we have an evaluation form at the end of our live seminars that people fill out and give us a scale on a 1-9 scale.

Greg Hughes: So more of a subjective rating kind of thing and different types of things like that that go into...

Chris Avis: Yeah...

Greg Hughes: As an IT manager or a manager of a variety of different kinds of people, you know, over time, it's always been interesting to me to find out how different types of employees or different types of workers are evaluated.

Chris Avis: Yeah, and we actually do more than just live events. We do a lot of webcasting. The bulk of us actually do some blogging. We do screen casting, podcasting. We integrate it with the community, with user groups, MVPs, so we touch a lot of different areas but it's almost always IT focused.

Greg Hughes: Well, having worked as a police officer before, I understand that quotas can be bad.

Chris Avis: Yeah.

Greg Hughes: And that there are many, many ways to actually judge the effectiveness of somebody in terms of how they are reaching out.

Chris Avis: Yes, absolutely.

Greg Hughes: And touching people that way.

Richard Campbell: All right, Chris. Exchange. I have a server. You have a server.

Chris Avis: Yes, I do.

Richard Campbell: We have spam.

Chris Avis: Ah. Well, I don't know. I may have less spam than you. I don't know.

Richard Campbell: I have a domain name that I bought the hard way, the old-fashioned way, in like 1993.

Chris Avis: Oh, wow.

Richard Campbell: And it's a three-letter domain name, which will remain unnamed. If you really want to know it, you'll be able to figure it out.



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

Chris Avis: Is it tla.com?

Richard Campbell: No, it's not. But the fact is, every single three-letter dotcom domain name is registered and I happen to own one of them and I've owned it for a very, very long time and it gets between 7 and 8 million emails sent to it a month.

Chris Avis: Wow!

Richard Campbell: So, I use it as my test case. When folks say they've got their spam under control, I say, "Are you sure? Are you really sure?"

Chris Avis: I'm in a similar setup. I've had a domain name for about 10 years. It's not a three-letter domain name. It's rather unique, but it's been public for most of that time, so friends, family have gotten it. They forwarded it out, it's gotten on the spam list and I get a rather fair amount of spam myself.

Greg Hughes: Yeah. I have a domain name that I use and my blog is at it and I've used it for a long time and there are days when I'm getting 2500 spam messages a day.

Richard Campbell: And we all agree the primary way that things get on spam list these days is scraping off of websites. Nobody sells lists anymore. None of that stuff goes on. The reality is the moment I put an email address on a webpage whether it's in a newsgroup forum that gets republished in HTTP or whether I actually put it on a page of any kind on my blog site, that's it, it's toast.

Chris Avis: That's it. It's public.

Greg Hughes: Well, that's one way.

Richard Campbell: Okay, Mr. Security Guy. While we're going after spam here. What are the other ways?

Greg Hughes: The fact of the matter is there are people who have email addresses that have never been put on a webpage and there's a variety of other ways that it comes up to. You're right, you're absolutely right that does happen. There's a lot of scraping that goes on but there are also worms that pull things out of address books and for the last three or four years especially, there's been a huge number of spams that are just sent to email addresses that are randomly generated, common names or other common monikers if you will at any existing domain name.

Chris Avis: Yeah, email's cheap to send so if you write an application or bot to just generate

random names, take the common, you know, john@company.com.

Greg Hughes: Right, absolutely.

Chris Avis: Then just start sending, it will get there.

Greg Hughes: That's why, now, depending on who you believe or ask or read, anywhere from 90% to 98-99% of the email crossing the Internet today is said to be spam. I don't know what numbers you have but it varies depending on which study you look at.

Chris Avis: Well, any way you look at it, every year since the Internet exploded a decade ago, those numbers have gone up. Ten years ago, when we look at it historically, spam was a nuisance. You get an email from someone that said, "Hey, look at this cool website." Now, it's the transport mechanism for malware, viruses, spam, phishing scams, and that percentage, because it is so cheap and convenient to send, the "bad guys," take advantage of that.

Greg Hughes: I mean you get a 1/1000 of 1% hit rate.

Chris Avis: Yeah.

Greg Hughes: You can make big money doing that and the fact of the matter is the reason that people do it is because they do make money.

Chris Avis: Yeah. Spam isn't there just because people have free time to send junk mail around. They are doing it for some gain whether it is to get personal information, generate revenue of some sort, and like you said, 1/1000 of 1% versus 1 to 5, a billion email addresses, that's a lot of money.

Greg Hughes: And it can be quite a bit. Now, not only has the amount of spam as a percentage of total spam out there or email out there being spam gone up, but just the amount of email being sent has gone up, I mean, exponentially, and the problem is huge. I know that I experienced in the past problems with doing anti-spam of scalability issues. There has been a lot of progress over the last several years in that area in terms of combating the spam problem. So, what's Microsoft got going in terms of solving this type of problem?

Chris Avis: Well, I think our first real big success with fighting spam was with Exchange 2003 in the Intelligent Message Filter. It was a free add-on for Exchange and I believe it was included with Exchange 2003 Service Pack 2. It was integrated in and it gave the administrator the ability to define thresholds and assign what's called an SCL or a



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

spam confidence level against inbound email. It was an algorithm that was developed based off the SmartScreen technologies that were put into the Outlook application and it looks at a variety of things. It looks into the subject line, the different words that are placed there. It looks at the content. It looks at who sent the email, who it is sent to, the time of day that it was sent, because one of the things you'll notice is that you will get more spam between midnight and 8:00 a.m. than you do between 8:00 a.m. and midnight. All of those different things were part of this SmartScreen algorithm and they're transferred over to the server side so that we could block it before it ever makes it to the end user mailbox.

Greg Hughes: So, one of the goals I know that a lot of administrators set out to do is; "I want to keep it from reaching my Exchange Server ever in the first place."

Chris Avis: Yeah, keep it out of the database.

Greg Hughes: Microsoft bought a company with an awesome product called Sybari Antigen.

Chris Avis: Yes.

Greg Hughes: An Antigen for Exchange, an Antigen like as SMTP Gateway. These are products that I've ran before and I've been really, really happy with -- I'm not intimately familiar, not being the hands-on guy for the last several years with what's happened with that product and what's changed over time since that acquisition, but I'm curious.

Chris Avis: So, what we have now with Exchange 2007 is we still have the Intelligent Message Filter-type capabilities. We implement them a little bit differently. Exchange 2007 is now a role-based type configuration. One of the optional roles is what's called an edge transport server and it is the SMTP Gateway. There are no databases for mail storage but that's where we point our MX records for DNS.

Greg Hughes: Okay.

Chris Avis: So, inbound SMTP hits that mail or that mail server, that role is designed to do all the scrubbing. So, we do our anti-spam, anti-malware, and that's also where we would install our Forefront Security for Exchange product which is the evolution of the Antigen products. We would install that to the edge server leverage. It does more than just anti-spam; it does antivirus as well.

Greg Hughes: It might be good to maybe just give a quick explanation of what Forefront is. There's

a server component, there are other things, and it's sort of like Microsoft with SharePoint. It's not a program. It's a group of programs or family, if you will.

Richard Campbell: Right.

Greg Hughes: So, what is Forefront, why is Forefront, and what is the story behind that?

Chris Avis: The name Forefront alone is actually a group of security technologies so it includes everything from ISA, Internet Security and Acceleration server, to our new intelligent application gateway server product which is our Whale Communications acquisition to the Sybari Antigen type acquisitions, anything dealing with security and protecting our systems really falls under the Forefront umbrella.

Richard Campbell: So, it's all of the edge services. This is what your Internet is plugged into. These are the machines that probably have real IPs.

Chris Avis: Correct.

Richard Campbell: You want as few business assets on those machines as possible. If any machine is going to take a beating, it's these ones.

Chris Avis: Correct.

Richard Campbell: So, they're purely focused on their edge roles.

Chris Avis: Yeah. They do primarily live on the edge. We do have a product called Forefront Client Security. It is an actual client side service that does the antivirus, anti-malware scanning, runs on our Vista, XP clients.

Greg Hughes: Now, is this the same as OneCare, or is this something different?

Chris Avis: Well, OneCare is under the Forefront umbrella but it is totally separate from the Forefront Client Security products.

Greg Hughes: Because one of the frustrations that I had recently with OneCare is that I can't install it on my Vista 64-bit machine. It's not compatible. So, is the Forefront Client Security 64-bit compatible or how does that work? I ask because I went out to a consumer store and bought a laptop and took it home with Vista on it and it turns out it was a 64-bit installation by default. That's what I got. So I'm kind of curious what the options are that Microsoft has available in terms of doing that base level security stuff.



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

Chris Avis: I know for a fact we have a 32-bit client for Forefront Client Security because I've done testing and demonstrations around that. My understanding is that we also have a 64-bit or at least it's in development, so we certainly will have one but I have to actually check to see where we're at in that process, but absolutely it will be supported. It's being continuously developed so it's not going to be going away anytime soon.

Greg Hughes: So, to kind of get back on the Exchange track here, so Forefront on the Exchange side is about antivirus and anti-spam.

Chris Avis: Well, actually Forefront is about antivirus. The anti-spam features are actually part of the edge role and some of the core Exchange services.

Greg Hughes: So, it's a core Exchange role, it's built into Exchange, that capability?

Chris Avis: The anti-spam is.

Greg Hughes: The anti-spam.

Chris Avis: Yes.

Richard Campbell: So, I set up an Exchange server and I set it to this edge mode essentially where it's going to do the anti-spam work and that's part of Forefront technologies.

Chris Avis: No, actually...

Richard Campbell: No, it's not a part of Forefront?

Chris Avis: No, no.

Richard Campbell: Okay.

Chris Avis: When you get Exchange, you have the option of doing this edge transport role and the edge transport role is unique in that it has to live alone. It can't have any of the other Exchange 2007 roles, the hubtransporter can't be a client access server, it can't be a mailbox database. In fact, the edge role can't even be part of the domain. It has to be outside of the domain.

Richard Campbell: I don't have a problem with that. That's how I would configure it too, you know, the same way I keep my web servers out of the domain and so forth.

Chris Avis: Right.

Richard Campbell: This is the machine that's going to take the beating.

Chris Avis: Yes.

Richard Campbell: You want to minimize its ability to expose the rest of it. It's not always going to win. Some days, the machine loses and this is security in depth. Don't leave it with the keys when the wall falls down.

Chris Avis: Exactly.

Greg Hughes: It is the abuse abstraction layer if you will. That's really what it is.

Chris Avis: Yeah. This service is actually designed to sit out in the DMZ or in the perimeter. I still have mine behind a firewall that only allows Port 25 in and out for that particular machine.

Greg Hughes: Which is also smart.

Chris Avis: It's just a smart thing to do.

Greg Hughes: But it's probably worth pointing out, I know we've said it on shows before, but it's really worth pointing out. If inbound Internet connectivity of the email type is coming in and it is touching your Exchange server directly, then you potentially fundamentally have a problem right there.

Chris Avis: Yes, yes.

Greg Hughes: The whole point of this abstracting the capability out and having an edge service is to have a very limited set of Exchange apps and capabilities running on that server in a highly protected mode so that like you said, you don't have data stores or anything there on the database so that you can really and truly protect -- I mean email is such a critical capability and service in companies today. The information that is stored shouldn't necessarily be, I'll pontificate again, but the stuff that people send in email quite often is really inappropriate to the media and protecting that is really a very important thing.

Chris Avis: Yes. A gain, that's why we moved that edge role out in the perimeter. I've mentioned it can't be part of the domain so a lot of people think, "Wait a minute. Exchange requires Active Directory services so we can look up user account information, figure out where their mailboxes live, etc."

Richard Campbell: Yeah, but none of that stuff lives on that machine.

Chris Avis: Well, it does, but in a kind of a protected mode so what we do is when we implement that edge server, there's actually a subscription that's made between the edge transport server and our hub transport server and it forms a one-way replication of



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

the Active Directory objects that are needed to do the mail routing. We replicate it in only one direction so it only comes from the hub transport server that's behind in our corporate environment, behind our corporate firewalls. We replicate that information out to the edge transport service so it can make its routing decisions and then, from there, we just move the email. It does all the scrubbing. There are no databases so anything that's spam-related, we kick that off. If we've implemented Forefront as part of this as well, then we can get rid of the antivirus before they ever touch the databases. It keeps them small, keeps them manageable, keeps them completely out of the environment if at all possible.

Greg Hughes: So, where do you run the Forefront anti-spam for Exchange? Do you run it on the edge server or is it a separate machine typically that you would run it on? What's the configuration that you guys...?

Chris Avis: You would run it on the edge server. The edge server is an optional role, so it does not have to be implemented in any size organization.

Greg Hughes: Sure.

Chris Avis: If you chose not to, you can run Forefront on the hub transport server for Exchange 2007. And if you've broken the hub transport role away from the mailbox databases role, then you're still keeping it isolated. Exchange does have the capability with some of the roles to combine them so you can actually do a full Exchange deployment with a single server. In that case then, Forefront would be running on the hub transport role with the mailbox servers as well.

Richard Campbell: Maybe this is a little off the spam track a little bit, but I am thinking about the granularity there. Would the first thing you'd carve out of that single server mode be the edge or would you carve off the transport? I mean what is the limiting issue here with Exchange? Is it number of mailboxes?

Chris Avis: Well, you know, we're going to go off on a tangent here, but there's roughly a 4:1 ratio.

Greg Hughes: We never go off on tangents, by the way, just so you know.

Chris Avis: It's approximately a 4:1 ratio of if you have four 2003 Exchange servers now, you could actually manage that same server load with Exchange 2007 with one server. The big differentiating factor there is that Exchange 2007 is 64-bit only. We could throw more RAM at that machine, which means we can reduce the disk I/O

which is a big part of the performance that hits on the mailbox server. We can keep more of that information in memory, so it increases the performance of the server, so that would be the big differentiating factor there. As far as breaking roles off, as far as a particular order, I don't know that we have a published particular order to do that. We could either have all of the roles live on one machine with the exception of the edge which always has to be a separate machine or we can start splitting the Exchange roles out which you might want to do for load balancing or performance reasons.

Richard Campbell: And just to be sure here, these could be virtual machines so it could be one physical machine, a virtual machine running the edge service.

Chris Avis: It could as long as you have a virtualized environment that supports the 64-bit environment.

Richard Campbell: Right.

Chris Avis: So, yes.

Richard Campbell: There must be somebody out there who does that.

Chris Avis: Oh, yeah. There is a company, we'll call them out, VMware does support it and of course we'll support it with Windows Server Virtualization on Windows 2008.

Greg Hughes: On 2008, right?

Chris Avis: Yes.

Greg Hughes: Right.

Richard Campbell: All right, back to spam.

Chris Avis: Oh, yeah.

Richard Campbell: So, what is it that the edge product is doing that's different from the Intelligent Message Filtering?

Chris Avis: Well, it's not really doing anything different. We still do our connection filtering. We still can do the sender ID. We still can stamp that spam confidence level on the machine. The difference is that is isolated. We keep that role completely away from where the database is restored so, again, if that machine gets compromised, it's just that machine. It's outside of the domain. We don't have to worry about it having connectivity into the rest of the domain and being able to enumerate any of the domain...



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

Greg Hughes: Hey, you start thinking about weird payloads attached to email that we don't know about now and somebody finds some random, you know, hidden vulnerability, then of course it instantly becomes known across the world.

Chris Avis: Correct.

Greg Hughes: And people start sending emails with dangerous payload that, you know, somebody comes up with in the future and having that, again, abstracted away in a limited role in a controlled environment is really beneficial.

Richard Campbell: Ultimately, we're about protecting the mailbox because that's what users get upset about losing.

Chris Avis: Yeah. Two different things, it's the end users want their mail and they don't want all of the junk. The administrators want the databases to be manageable and small, if at all possible, which is, you know, growing more and more difficult considering what people use email for these days. They use it for file storage as much as they do it for email.

Greg Hughes: And the risk managers want to make sure that the system stays solid and that information is not coming, which causes improper information to go out.

Chris Avis: Correct.

Greg Hughes: So, there's a wide variety of benefits to having an isolated and divided environment and doing defensive depth, as they call it.

Chris Avis: Yeah, layered approach to security.

Greg Hughes: A layered security strategy, yes, so that you can have multiple layers of protection. Certainly, you wouldn't rely on just that edge layer, you would also properly secure everything in every layer below that.

Chris Avis: Absolutely.

Greg Hughes: Because it's quite often what you don't know.

Richard Campbell: All right. I'm not going to go dark on you. Yeah, I am. I'm beginning to think that email's simply broken and the biggest measurement that I've got is the regular mortals, I mean let's face it, we're weirdoes, right? We're in this space, we're trying to keep mail working, but grandma is using Facebook for her communication.

Chris Avis: Right.

Richard Campbell: Right? These social sites are becoming the way they're communicating because email is simply not working. My kids are giving up on email and using Facebook and using MySpace and things like that because they not interested in the battle. It's not important to them. They would rather message through something to their friends that they can count on.

Chris Avis: Well, you know, I would say it's not even so much the reliability of email itself, it's just that as the Internet and as the different applications have evolved over the years, and particularly in the younger generations, using the applications, the social networking sites like Facebook, MySpace, etc., they have that built-in messaging capability. I wouldn't even really call it truly email. In fact, on MySpace, you have comments then you have new messages. I don't even think the word email actually shows up, but it essentially is. It's a messaging environment and there is a certain amount of migration away from using a full-blown email client in some environments.

Greg Hughes: Well, you know, email sucks. It's broken, it's always been broken. It was broken from the day that it was designed. It's a lot like TCP/IP, you know, well-intentioned people who believe that all the people in the world are kindhearted and good and would never do wrong built optimistic applications that do a really good job of doing what they're intended to do. The problem is that they're also open to people using them in ways that they were not intended, right? And doing bad things with them and the fact of the matter is that when the Internet sort of hits it boom 12, 13 years ago, when it really started to grow and it really started to take off, you didn't have a whole lot of bad guys out there taking advantage of it. Now, you have, you know, zillions of them and they're really, really good, very smart people. Fundamentally, email is a broken media and that's why you do see, I mean I agree, I don't think email's dead. It's far from dead, unfortunately, but you're right. People are using things like Facebook or instant messaging. I use instant messaging a lot now to communicate with people; and I have for years. I'm using it more and more because more and more other people are getting on board and are using it as a regular way of communicating with each other.

Chris Avis: Yes.

Richard Campbell: All right. I'm going to try and keep us on spam to some degree here, but you know, these are -- the funny thing about spam is we deal with it from an IT perspective but also very much from



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

a personal perspective because we all use it as well, so it's a fairly tough topic to focus on abstractly. It's a very non-abstract problem. We only talk about this concept of intelligent message filtering, about looking at the criteria of the message itself, decide if it's spam or not. What about stuff like blacklisting? The other mechanisms around -- and I'm talking about blacklisting servers. I know perfectly well from my experiments that if I fire an SMTP open relay on, it will be found within minutes. I've got a few extra IPs out there, I've done this as a demonstration where I've literally just set up a simple SMTP server and put it out open and within minutes it was found. There are guys out there scanning for 25, round the clock and it was a mail relay and it was immediately compromised. I mean it was a stunning demonstration. So, the issue here is blocking those servers and then the next thing was within an hour on a blacklist.

Chris Avis: Yes.

Richard Campbell: We've obviously got a group of people out there who were trying very hard to make blacklist work but I see people in both camps. I wonder where you are in this, Chris. Do you use those technologies?

Chris Avis: Yes, I do. I've been doing this with the blacklisting, the DNS blacklisting since Exchange 2003 and I've actually posted it out to my blog on several occasions. I'll rotate through different blacklist providers over time because I actually have about 30 domain names total that are registered. I only have a few of those enabled for email though, but I leverage connection filtering so there are specific IPs that I found through my own network tracing, etc., and just monitoring things over the years that I know are known spammers, known virus senders, etc. So, I put into the connection filtering those IP addresses. Since Exchange 2003 has supported DNS blacklist providers, where you can plug in the name of the DNS or a hosting provider that maintains a DNS zone of known spammers, virus senders, hackers, etc.

Greg Hughes: A lot of times, they are referred to as a real time black hole list or RBL list, those types of things. I think it's important to mention to people since we've started talking about that, that there are a few RBL list out there that are probably pretty good to use and there's a bunch of them out there that are extremely aggressive and will cause you more problems than they will solve.

Richard Campbell: RBLs are lovely and spam-filtering is lovely until you get false positives.

Chris Avis: Yes.

Richard Campbell: All of this is fine until a guy doesn't get a mail he knows he was supposed to get and now you're in trouble.

Chris Avis: That one situation is -- people over the years have figured out, people would much rather get 10 spams a day than to have that one email hit as a false positive and then not get it.

Greg Hughes: Right. The quandary that we find ourselves in is would they rather get 500 spams a day or miss that one email? Would they rather get 1000 spam emails a day or miss that one email?

Chris Avis: Yeah. What's the threshold?

Greg Hughes: I mean you're right. You're absolutely right that it's the inconvenience balanced against the other inconvenience.

Chris Avis: Steve Riley did a good keynote around security versus usability. I'd heard the presentation before. It's very good. The same thing applies with the spam side of it, you know, where do we set our thresholds for how much spam we're going to allow in to guarantee that we get our valid emails versus what we want to block and take the risk of eliminating the valid email from our system.

Greg Hughes: You know what's interesting too is a huge amount, a very, very large percentage of the email can be dropped right upfront based on invalid SMTP headers and forged sender IDs, right? I've set up a wide variety of different types of anti-spam engines and gateways just to do analysis and to learn about that and the vast majority of spam is so badly formed. I'll say this here and then they'll hear and say it and then I'll go out and try to fix it. No, they won't because they haven't fixed it for years.

Chris Avis: No, they haven't.

Richard Campbell: You get back to the point, which I think of the spammers is a very small subset that are pro, that are handling the viruses and doing the phishing attacks and so forth, but there are all these kits out there that anybody can download to be a spammer. I just love getting a spam where the subject line is insert subject here, right?

Chris Avis: They forgot that field in their little kit that they did.

Richard Campbell: And it's almost like they don't even know what's running anymore. It's a runaway themselves.

Chris Avis: Oh, there's no doubt in my mind that, you know, some years ago, some hacker bad guy set up a machine to start sending some



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

spam out and forgot about it and it's been spamming. It's like the theory of the whole Novell server they got walled off and it ran for 10 years before something happened, knocked the wall down, same type of thing. It becomes an automated process and the bad guys have written little applications that make it so simple for the script kiddies out there go out to some site, download a utility plug-in if he feels, press go and instantly, they're sending millions and millions of messages.

Greg Hughes: Right, with the advent of bot networks where we start to distribute those across thousands and thousands of different sources where they are all coming from and to make it harder and harder to track but it's encouraging at least to know that there's still great progress being made by Microsoft, and by a variety of others. They're doing a very good job and quite often working together on these things and collaborating idea-wise on these things, these conferences that everybody goes to and shares information in order to be able to basically draw up as much of this as possible at the edge.

Chris Avis: Yes.

Richard Campbell: I'm still surprised at technologies that have never taken off like authenticated mail. I mean, once in a while I get a mail from somebody with a little symbol on it but why have none of these things taken home?

Greg Hughes: Because it's a pain in the ass.

Chris Avis: I think that's what it is. It's cumbersome.

Greg Hughes: It's usability versus security. Security measures are good but the fact of the matter is people won't use them if they don't work.

Chris Avis: If it takes 5, 10 clicks to set it out and then any kind of monitoring after the fact, it will not get adopted by the customer.

Greg Hughes: Especially if every time you send an email you have to sign it through this geeky, techie way of doing things. There's a difference between it works and it works for me.

Chris Avis: Yes.

Greg Hughes: Really, that's the usability question and this'll go back to your point, I think that as soon as something becomes more usable, then it will be adapted but to go back to the classic email, the way that it is architected and works today doesn't anticipate and doesn't really, in a usable way, allow people to do authenticated email or to have email that is really just following certain channels.

There's a flipside. I mean one of the beauties of email if you can call it that is that you can reach anyone anywhere in the world unimpeded. You can just send it unless the government gets in the way or something, but I mean, technically speaking, it's very fast, huge amounts of information and it's unimpeded. You don't have a list of friends that will accept your email.

Chris Avis: Correct.

Greg Hughes: If you want to reach somebody you've never spoken to before because you're curious about something they wrote, you can just do that.

Chris Avis: Yeah. I get that all the time. I mean I blog, my email address is on my blog. I get email from all over the world from people I've never spoken to ever and they have questions about something that I've posted or some webcast or something and it's very easy to establish that two-way communication with unknown people. I've got friendships that I've had for 12, 13 years since the boom of the Internet with people that I've run across through some web form or something and email communication I've never met some of these people, but we've talked for years.

Greg Hughes: I mean email was the original social network, right? Then instant messaging came in and so there is a value in that, but there's also cost in having an application platform, if you will, that works the way that it does when the bad guys try to obliterate it. They've just done a pretty good job of doing it.

Richard Campbell: Yeah. I think my email is pretty close to obliterated.

Chris Avis: Well, it depends on how you look at it. I mean if we have a few minutes I can tell you a five-minute story about spam and some stuff I did to save my marriage.

Greg Hughes: Absolutely.

Richard Campbell: I love it.

Chris Avis: We talked about this earlier.

Richard Campbell: Let's do it. Let's close on a good story.

Chris Avis: Yeah. So, I've run my own Exchange server for about 10, 11 years now.

Greg Hughes: And that will kill a marriage.

Chris Avis: That in itself. Well, all the machines in the basement I think is what it does,



Chris Avis fights Spam on Exchange Server 2007!

December 5, 2007

but... And I've had this domain name for many, many years and my wife and I, she's had an email address on the domain for about seven years now and it was running Exchange 2003 up until six months ago and had the intelligent message filter on and she was seeing maybe a dozen spams a week total and almost all of that ended up in her spam folder, her junk mail folder, so I convinced her that I had to go out and get the 64-bit machines to do Exchange 2007 if she still wanted to get email and she did. She wanted to get her eBay notifications, communicate with her friends and family, so she let me get the machines and I install and migrate everything over from Exchange 2003 and got it all up and running. Notice all of the spam coming in, didn't really give it much thought and then I went on the road and I was on the road pretty constantly for about six months and also got a little bit lazy. I don't use my personal email address much anymore. She does though and she actually got into the routine of every single day, she had a thousand mail messages in her inbox, which I didn't even realize. She would just do a CTRL+A to select everything, do a delete, then she would go to the deleted items folder and she'd start running through it to find the valid email and then she would say "mark as not junk" to start creating a list. I had not configured any of the anti-spam features inside of Exchange. That's what the message or the key was. So, her email address was getting about a thousand spams a day. I was getting somewhere between 1500 and 2500 a day and I was amazed I didn't even realize that. I'd quit monitoring the spam in my servers since doing the intelligent message filter, the blacklist connection filtering, because I was getting almost no spam. So, after six months, she finally puts her foot down and says, "Look, I'm getting 7000 emails a week. You have to do something about this. I cannot keep up with it."

Richard Campbell: Get back to the old server. The old server didn't do this.

Chris Avis: Yeah, she said, "You got a \$1000 budget to go out and buy a couple of 64-bit machines. You built them and my life is horrible as far as email is concerned, so you lied to me," is what she came down to. She finally put her foot down and I said, "Okay, look. I'm gonna do this whole other server. We'll get it up and running." So, over the weekend, it doesn't take long, I implemented the edge server role. I also implemented Forefront because I wanted to do the antivirus part of it as well.

Greg Hughes: Right. Sure.

Chris Avis: Because I deal with a lot of security as well, so I know that's one of the transfer mechanisms and we instantly went from a 1000 spams a day for her, roughly 1500-2000 for me, back down to the pre-upgrade levels where she's actually

getting maybe a half a dozen a week because I've implemented a few of the other features that Exchange 2003 doesn't support.

Greg Hughes: Some of the newer tweaks?

Chris Avis: Yes, some of the newer tweaks. I actually configured sender ID. I haven't really done any testing to see how much that's blocking, but Exchange 2007 with the edge services also has this reputation item as well that can look at the reputation of the server and actually if it says "Yeah, it's kind of sketchy," we're going to block all the incoming connections from that server for 48 hours and then we'll allow some connections in. We'll check the status of it then and if it is still sketchy, we'll block it for another 48 hours. You can enable some logging to see how that's doing and then go in and make some connection filtering list. But she was very, very happy to say the least of getting back to the pre-upgrade to Exchange 2007 levels of spam and it just really opened my eyes. That's one of my domains that I was doing email for.

Richard Campbell: You've forgotten that your stuff was actually working.

Chris Avis: Yeah. I mean it was very transparent so when we say email is broken, it is because it can be taken advantage of so easily by the people that have less than good intent. On the flipside, I really think that with proper administration and configuration, regardless of whether its a Microsoft mail system or even third party, jumping through some of those fiery hoops of fraud will really make the lives of our end-users and the administrators a lot simpler.

Greg Hughes: Clearly, there has been a lot of investment and effort.

Chris Avis: Absolutely.

Greg Hughes: Put into making email work better in the current environment, but to Richard's point, eventually something will come along and it will see some adoption that will replace email just like the automobile replaced the horse, you know. It will eventually be outwitted and out-developed and something better will come along.

Richard Campbell: You don't see a lot of Archie and Gopher these days.

Chris Avis: No, no, we don't.

Greg Hughes: That's a good point, but despite the fact that spam is terrible and that phishing and viruses attached to email and the worms and all the



different stuff that can go on in email so bad, people still use it because it fundamentally meets a need.

Chris Avis: Yes, it does.

Greg Hughes: So, until something else comes along to meet that need, then it's important that Microsoft with the Forefront stuff and other companies that are doing this are doing the hard work they are doing because it does add real value to an awful lot of people every single day.

Chris Avis: Yeah. There's no one that I know that has any kind of Internet access that does not have an email address. I kind of wig out with people that say, "Oh, I've got 10." I'm like, "That's crazy. You have 10 times as much spam as having one." I have two email addresses. I have my work email address and I have my personal email address.

Richard Campbell: Right.

Chris Avis: I've been that way for a decade now. I can't imagine having one more mailbox. Oh, I should take that back. I do have a Hotmail account, but it's locked down. I don't allow anything into it at all. It's just for my Windows Live ID, but I have my two email addresses. That's it. That's all I want to have to worry about and I use both. Well, I use my personal one a little bit more than I did six months ago, but my work email is probably my primary messaging area.

Richard Campbell: Chris Avis, thanks again for your time. We really appreciate you talking to us.

Chris Avis: Absolutely.

Richard Campbell: Fun to do this at the conference and I'm sure we'll all be together again sometime soon. And we'll talk to you next week on RunAs Radio.