

## Management & security issues for Cloud Computing

*Date: Fri, 02/26/2010 - 13:31*

Cloud computing services are being touted as a panacea, as a way to flexibly deploy services and reduce costs. But what is the reality when it comes to security? How can enterprises properly evaluate cloud-based security offerings to ensure they truly support an appropriate security architecture, as well as consistently offer acceptable protection levels and response times? What assurances and metrics exist to protect sensitive and personal information? Are these services equal to, better or worse than the alternatives, namely on-premise managed security services or in-house enterprise security practices?



Nikki Babatola, analyst from Canalys

Nikki Babatola, analyst from Canalys, explained at NetEvents EMEA Press Summit, in Barcelona, the significance of Cloud Computing

**Panellists: Steve Broadhead, Founder & Director, Broadband Testing; Rik Ferguson, Senior Security Advisor, Trend Micro; Bo Fjelkner, Principle, Nordics Sales Engineering, Verizon Business**

### **Nikki Babatola - Canalys**

What drove the interest in cloud computing? People are looking at their IT budgets. People are looking at their IT costs. And they certainly saw cloud computing, or SAS, so far as a service, as a way of reducing some of those costs, as a way of moving from capital expenditure to operating expenditure.

So we did a couple of surveys, first through the channel. And we asked channel partners, this is resellers, systems integrators and distributors, "How important will cloud computing be to large business customers by 2011? And over 63% of respondents said it was going to be very important, too important to customers.

So clearly, this is a big interest, for not just the end-users but also the channelers. They see this as an opportunity for growth in their revenues as well.

And we also did a survey of 600 enterprisers -- this is a mix of small businesses and large businesses, asking them how their ICT budgets were going to change in the future. And this is, I think, how it was going to change in 2010 and 2011. And this is a selection of some of the comments we got. We said, "We'll invest a larger proportion of budgets in outsourcing some of our ICT requirements." So obviously, outsourcing to service providers but also integrating some of that infrastructure to the cloud. We got a comment, "Increase outsourcing and offshoring. Increase SAS." So again, there is that trend of moving a lot of the software into the cloud, of taking software or taking services from service providers as well.

So there are a lot of benefits, primarily cost benefits, in moving to the cloud, simplicity of moving to the cloud. But there are several security issues of moving your infrastructure, data and software into the cloud.

Reliability. A lot of these companies that offer these services are start-ups. So how are we sure these companies are going to be in business going forward? How are we sure they're not going to be acquired by a larger company? Are we sure that they're not going to go bust? So reliability or the sustainability of these companies is an issue for a lot of companies. The reliability of getting access to that data, as well, is a big concern to a lot of companies. If I want that data, am I sure I can easily get access to it? Will it be available?

You have access control problems. So putting my data into the cloud, who gets access to that data? Are there any parameters, assurances, as to who is going to control that data, who gets access? And can we measure who gets access to that data in the cloud as well?

We also have data-loss problems. Putting this data in the cloud, where is it being stored? Who has access to it? This data can be lost, so of course that's another problem for them, and compliance and regulatory issues as well.

And again, another survey that we ran, asking channel partners. We said, "What are the barriers to growth in cloud computing?" And behind expertise of both the end-user and the channels, security concerns was seen as a big hamper to growth for cloud computing, for the channel.

So a lot of vendors and a lot of service providers have realised that these security issues are hampering growth and are slowing things down for them. And we're seeing a lot of vendors develop their capabilities in protecting cloud computing, and service providers putting more encryption and more protection mechanisms into their cloud infrastructure.

But we're also seeing a whole host of security vendors acquire security-as-a-service vendors to also provide, not just security for cloud computing, but security from the cloud. So, for example, we see Trend Micro acquire Third Brigade, to provide capabilities in vulnerability management, to provide capabilities for enterprises. We see Symantec acquire Message Labs to provide Web and email protection from the cloud, as well, to customers. And we expect this trend to continue, for vendors to provide protection from the cloud.

So going forward, we expect network security, for example, to come from the cloud. We have this hybrid model of cloud computing. So I've put some of my infrastructure in the cloud and I've got some of this physical infrastructure as well. How can I manage that security of the cloud computing infrastructure and physical infrastructure?

We expect vulnerability management to move to the cloud. So there is a lot of management required in patching these systems and in checking the vulnerabilities. And we expect that this too will move to service providers in the cloud, so that these companies can focus on more strategic technologies.

So I think this panel is just really to address some of these security issues, to look at how vendors and services providers are protecting enterprise data and protecting enterprise infrastructures.

So I think, to start off with, it would be interesting just to get a quick introduction from you guys and a quick insight to how each of you are protecting or are involved in cloud computing security. So if we start with you, Rik.

### **Rik Ferguson - Trend Micro**

My name is Rik Ferguson. I work for Trend Micro. And we're involved in the cloud in a couple of different ways, really. So something that we launched two years ago is called the Smart Protection Network. And this is providing security from the cloud. So we were able to enhance and improve, offering and change completely the way that we detect malicious activity and malicious software, by moving what's normally stored, or traditionally has been stored, as local pattern files on each individual endpoint, to a dynamic, real-time query-based system in the cloud, and integrate intelligence on malicious files, malicious URLs and malicious email information into one real-time query database. So we can provide more effective, more rapid protection to our customers.

So that's how we use the cloud for our own services. On the other side of the coin, if you like, is protection for the cloud. And for that, obviously we made the acquisition of Third Brigade last year. And we've developed some in-house stuff as well. So protecting for the cloud -- we need to stop thinking about the cloud because it doesn't really mean anything. Or more accurately, it means different things to different people.

What do we need to look at, in terms of protection, what are the motives that drive the cloud? And for me, some of the most important ones are virtualization, multi-tenancy and storage area network. So those are three of the biggest engines that are powering cloud [invasion]. So that's what we're looking to protect. With our Deep Security product, we're looking at allowing people to do what we call virtual patterns. So they can run their services un-patched but invulnerable, if you like and create

patch windows, because a cloud environment is one that needs a large amount of uptime. You need to be able to manage your patching windows effectively and say, "I need time to collect all the various patches from the vendors that don't have a joined-up schedule, group them together, create a patch window, test them beforehand and then deploy them." But know that during that window, I'm not going to be vulnerable to attack because I, the cloud provider, am providing an important service to my customers and must be able to [pre-confine] the service. That's how we're involved in [security] for the cloud.

### **Steve Broadhead - Broadband Testing**

So actually, we do product testing, including, in fact, Rik's product which we probably can touch on. So what has been interesting for me, because I test hardware and software, is to see the change in the last four or five years with what we call Web service-based application, i.e. talking to a TCP port rather than actually a specific, powered physical location.

And an interesting point, even then, from about four years ago. I also do due diligence work with venture capitalists. I remember meeting with a guy from [31] in London about four years ago. And he said, "We're only going to invest in software as a service." And that was four years ago.

So if anyone doesn't believe in the whole cloud thing, that it's going to happen, because there's just too much behind it for it to not happen. It's more or less being forced on people. So my role is to see if this stuff actually works, basically.

### **Bo Fjelkner- Verizon Business**

My name is Bo Fjelkner. I work for Verizon. And what we see is a trend towards everything as a service. And our heritage is coming from providing services, way back in time. Security as a service is one of the fundamentals within our company. We acquired CyberTrust some years ago and that has been totally integrated in the company. So security as a service is one of the keys, then [for us] to enter the cloud and what we are doing in that space.

### **Nikki Babatola**

So what are some of the security challenges you see then, or you think enterprises need to assess before actually moving software or infrastructure to the cloud?

### **Bo Fjelkner**

First of all, probably one has to start looking at what one has today. When you move over to a cloud solution, the main concern is around security. But perhaps the first step is to know what type of security you have today. What we provide in our computing as a service which is the official name, it's actually following our stand that within security, what we are telling our customers to do, in terms of security, having a layered approach, etc., that we implemented in our computing as a service solution.

### **Nikki Babatola**

Steve, what do you think are some of the challenges companies need to think about, in terms of security, before moving to the cloud?

### **Steve Broadhead**

I think we need to differentiate between a large enterprise .... An enterprise, obviously, is going to have a much bigger understanding of what it actually means to put everything in the cloud and the issues of being able to access that. Is it really secure? Is there data actually being shared on the same server as someone else's, etc.?

For a small-medium business, I don't think they actually care because they pretty well outsource everything already, to a service provider. And it should be completely transparent to them.

### **Nikki Babatola**

But I think even for a small business, it depends on the vertical as well, because you have very specialised verticals, who can't afford to lose their data from the [cloud].

### **Steve Broadhead**

Well sure, if you've got real high-value, and particularly if you're thinking in terms of very high-value stuff, like video guys, legal, etc., especially yes. But that is a slightly different concern. So I think you

have to separate it even further, into different verticals and say, "What are the issues there?" And there is a whole list of what happens if, and we could spend all day talking about those.

**Nikki Babatola**

And Rik, from your experience with large enterprises, what are some of the primary concerns that they have in trying to move to the cloud?

**Rik Ferguson**

For large enterprises, it's a similar problem with cloud. Cloud means different things to different people. And security means different things to different people as well. And that's something we have to keep in mind. If you ask a sys admin, or a network admin, or a coder, or a hacker, or a three-star general what security means to them, then you're going to get a different answer every time. So for large enterprises, I guess the person you need to ask the question to about what is security, is probably the C-level executive because they're the people who are ultimately either going to be pushing for or pushing against the cloud. So for a C-level exec, I would say that security is all about control and accountability. If you have control, then you're willing to accept accountability. If you don't have control, then you're much less willing to accept accountability because you can't influence events. Now with the move into cloud, the big problem in most cases is that you outsource much of the control. But legally, you can't outsource any of the accountability. So that's the problem that we have to solve. We have to make sure that the data controllers, the data protection, but they took control as data owners, intellectual property owners, retain control of their property, all the while moving it into the cloud.

**Nikki Babatola**

Well there is a lot of focus on some of the downsides of moving to the cloud for security. But surely there are some benefits, security-wise, from moving to the cloud as well. I guess central policy setting, those kinds of things might be a benefit. So what are some of the benefits you would expect to be realised from moving to the cloud, for enterprises?

**Steve Broadhead**

For enterprises, it's difficult. Certainly for smaller businesses, there are many, many infrastructure benefits because they don't have the capital to invest in the hardware and the systems that larger enterprises already benefit from.

On an ongoing basis, obviously the biggest benefits to large enterprises are going to be cost related. It's not particularly going to be security related. It's going to be about [greening] IT and it's going to be about not having to reinvest CapEx in buying new firewalls and new appliances and whatever it might be.

**Nikki Babatola**

And from your experience, Bo, what do you think some of the benefits have been, from what you've seen of enterprises moving to the cloud?

**Bo Fjelkner**

One of the benefits is that you get implemented the best practice that we are promoting. You can read in the [Data Breach] report from the Verizon business where, it's the fifth year now, we are outlining what is happening on the cyber-crime space. And knowledge is then implemented into our security as a service offering. And as I said, that ties into all our offerings. You get it automatically in other offerings as well. You get best practice implemented.

**Nikki Babatola**

And Steve, what security features then, from testing these products and working with these products, are vital then, that need to be put in place to move to the cloud? Are there things like data protection, or do you find that vulnerability management and patch management is increasingly important?

**Steve Broadhead**

It's all of those things. But if you go back a step, first, talking about the obvious benefit, in theory, the cloud, it's back to the old centralised versus distributed argument. So we had the mainframe. And then people went to PCs and that worked. So everything got distributed. And they went, "Oh, that's

unmanageable. We'll move back to the mainframe." And basically what the cloud is, is effectively a virtual mainframe. The only issue is, you don't have the control of exactly where that data is. But in theory, from a cost perspective, like Rik says, it should save stacks of absolutely enormous amounts of money. It may put some security vendors out of business as well because the issue is, if you've got this [lead] security [ring], you've got one, two, three four, five, six, seven, eight appliances within the LAN, on the edge, within the boundary out, etc., that also is pretty well unmanageable. So the logistics of actually having everything up there and just having a single access point is fantastic. So then we go into an example. When I actually reviewed their OfficeScan 10 product last year, what I chose to do as part of the test, I took a regular non-cloud-based security product from another well-known, slightly Irish-sounding company. And I was travelling around England for a month. And I had two laptops, because I'm really sad. And I was doing a lot of stuff on the train. I had two 3G dongles. And so on one laptop I had the OfficeScan 10. It's a very small footprint, so you just have a very tiny database -- and Rik can go into more detail about that -- on your laptop. But essentially, it's cloud-based. And on the other, I had another traditional solution, shall we say. And this was the issue I found as a user, which was a fantastic positive for cloud-based. On those rare moments when I actually got a strong signal on 3G dongles -- I'm on the train down to Brighton before you start hitting all the tunnels [inaudible]. And you're just desperate to get some emails out. Guess what? The other one starts downloading the latest update. And it just completely chews up every bit of bandwidth you've got. So that laptop was completely unusable. The one with OfficeScan 10 -- and I'm not using this as a promo but it really did work -- was fantastic. Am I protected? Absolutely. Did it find as many viruses, etc.? Well of course it did, absolutely.

#### **Nikki Babatola**

I guess the question was security as a service. And that case then is if you don't have that Internet connection, how does it affect your protection level? Are you still protected?

#### **Steve Broadhead**

Well yes, you are because fundamentally, apart from internal threats, practically every threat is coming from the Internet anyway. So if you're not connected to the Internet, then the threat protection level is that much lower anyway. But yes you are.

#### **Rik Ferguson**

The easiest way to characterise that is to say that if you're using a traditional anti-malware solution, which we still do as well because there are people that want it. But if you use a traditional anti-malware solution and you're not connected to the Internet, then the protection that you have installed on your local machine will slowly go out of date and you will end up not being protected. The same is true of the cloud-based system. There is no difference.

#### **Nikki Babatola**

So just going back to that question then and Bo again, from your experience, what are some of the security requirements that are needed before you deploy, or move infrastructure to the cloud or move software into the cloud?

#### **Bo Fjelkner**

Coming back to the best practice and so on, one of the things we see from talking to customers is that we had to convince them about how our best practice is implemented. And one of the things I was using is, for instance, with accessing servers. How does a customer today do it when they're accessing their servers? Are they going directly on their servers? And quite often, that's the case, whereas with our computing as a service offering, we have layers, so any one of our IT technicians, when they do patching, it works on the servers. They go by a layer. So we are logging everything they're doing, not to control them, but to make sure that we can trace if a mistake was done. That type of discussion, then, helps the customer to realise that, oh wait, moving into our cloud, or computing as a service is perhaps adding a security level that they might not have in existing services.

#### **Nikki Babatola**

Which helps with compliance with regulation if you are tracking who is getting access to what and from where. But then how does that tie in with some of the dedicated security products that you guys

and Trend Micro have? Do you feel that just having that tracking is enough or do you still need that protection, like you said, of virtualisation security, data protection and so on?

**Rik Ferguson**

Yes. Obviously that's fantastic best practice, absolutely. The problem is, for cloud consumers, people that are going to cloud providers, that most of the services employ virtualisation to a greater or lesser degree. And there are many issues that are raised by virtualisation, which didn't previously exist. So virtual servers are vulnerable to all the same threats as physical servers. They don't go away.

But in addition, we get some new things. And one of the most interesting is the threat from traffic travelling between virtual machines on the same host, because your traditional architecture is not able to mitigate against that, because it doesn't hit the wire. So you're on the wire IPS. You're on the wire firewalls and not going to see the traffic travelling between VMs on the same host. And that's one of the issues that we try to resolve with Deep Security, by implementing a virtual appliance that hooks in with VMsafe and is able then to manage traffic between machines. So if somebody brings up a rogue VM on the host, or if somebody brings up a poorly-configured vulnerable VM on the host, you can be sure that that's going to be segmented away and your stuff on the host will be protected.

**Nikki Babatola**

And is that capability only for VMware right now, or do you have capabilities for [Citrix] and Microsoft, for example?

**Rik Ferguson**

So the Deep Security product, in general, is Microsoft, Citrix, VMware. It's multiplatform. The virtualised appliance is using VMsafe in particular. But we're looking at doing stuff with [Zen] as well. The other thing that we're doing, the second part of that, is around data protection. And it's about enabling people who are using, I guess more software as a service type cloud offerings, to place encrypted data in the cloud. And only they have the keys to that data, because one of the big problems when you're consuming cloud services like that is what happens to your data when you switch providers? How can you be sure that your data has been deleted? How can you prove security of your data when you've gone from provider X to provider Y? If you know that the data you put in the cloud was encrypted anyway and the only person that has access to the keys is you, then that becomes much less of a problem and much easier to demonstrate compliance.

**Bo Fjelkner**

And these types of solutions, implementing into our offerings and so on, we do see a problem from customers asking about this issue you're just describing. And this, what you describe, is helping you to argue. Some of the customers will not be convinced anyway. Then we can do, in our computing as a service offering, a physical server, so they get a physical server. End of discussion. But it's definitely an excellent step forward, having this possibility that you provide.

**Nikki Babatola**

And Steve, just to touch on your point that you mentioned earlier then, whose role is it to protect the enterprise or to protect the cloud computing infrastructure? Is it up to the service provider or is it still up to the security vendor? Who is going to go out of business?

**Steve Broadhead**

Yes, that's a very good point because what I was going say, now that I think of it, is that I don't think that the issue is basically building the virtual equivalent of some physical devices and appliances. But in that virtual world, it's what happens if something goes wrong. Who do you point the finger at? Do you point it at these guys? Do you point it at these guys? Are you supposed to take responsibility yourself? Should there be some government compliance? I'm not saying along the lines of Sarbanes-Oxley. But basically, this is a completely new trust requirement between customer and vendor. And I think it's a grey area, completely at the moment. I don't think anybody has really given some proper guidelines as to how this should work.

**Nikki Babatola**

Well what's your opinion on that, Rik? Do you think it's up to the security vendor or should the service provider include more security capabilities into their offerings?

**Rik Ferguson**

I think we just need to look at what the current state is. So under current legislation in most countries in Europe, the data controller is responsible for the security of the data. And that's the end of the story. You can blame whoever you like, but legally you're responsible. And that's the way it is and that's the way it's going to stay.

**Nikki Babatola**

So it's up to the enterprise.

**Rik Ferguson**

Yes. And also, if you look at the terms and conditions offered -- I don't know what yours are -- but by the majority of cloud providers, you could condense them into a single sentence that says, "We don't guarantee this stuff works and we don't guarantee it's not going to break." And I don't think that's going to change, either.

**Steve Broadhead**

How many guys does that actually potentially put off, Rik, enterprises moving there, because you say you've got to take full responsibility regardless, right?

**Rik Ferguson**

It's no change. There's no change till now. They take full responsibility now. They're going to take full responsibility in the cloud. It's not different.

**Steve Broadhead**

But are they going to accept that, the fact that they've got to do that when they --

**Rik Ferguson**

Yes, I think they are. At the end of the day, the security guys are not going to be the people who are going to make the decision whether to or not to go to cloud. It's business is going to drive it into the cloud. And they're going to see cost reductions. They're going to see lower CapEx. They're going to see greening IT. They're going to see all of those benefits and say, "That's what we're doing now. You guys work out how we can do it securely because we're doing it anyway." That's what's going to happen.

**Nikki Babatola**

From a service provider perspective, then, do you see yourself increasingly including security into these capabilities? Or again, do you think it's up to the enterprise to try to secure these deployments?

**Bo Fjelkner**

I think one can look at PCI compliance. We can help a retail customer be PCI compliant. But then [inaudible] a customer that are PCI compliant. So it is a relationship between the customer and us, of course. But in the end, it is the customer that is responsible. We have SLAs and all those types of things. And that's important. But responsibility is very much with the customer.

**Steve Broadhead**

Because what is your SLA going to say? It's not going to say, "And if we mess up, we'll go to jail for you." You can't do it, can you?

**Nikki Babatola**

I'd like to open it up to the floor now. Do you guys have any questions you'd like to ask the panel?

**Toni Eid - Telecom Review**

Why we don't apply the same procedure at the corporate server, instead of giving to cloud and losing control and all those things? The security, everything done by the cloud, why don't we do this on the server to keep the control and keep the security aspect local?

**Rik Ferguson**

In Trend Micro terms, the technology that we offer is designed to be used inside your private cloud,

your personal data centre, hybrid cloud, public cloud, virtualised infrastructure, physical infrastructure. You can use it where you like. The only reason I'm relating it to cloud is because that's what we're talking about. But it works everywhere and we recommend it everywhere.

### **Bo Fjelkner**

And may I put in a comment there? It is possible to read our database report and learn about what we are recommending, in terms of doing it on premises, using equipment and so on. The advantage of doing it in the cloud or a securitised service is flexibility. You have a proper SLA between us and the buyer, within the customer side. And I think there is a cost advantage actually, doing a securitised service.

### **Toni Eid**

Cost advantage, percentage-wise, how much?

### **Bo Fjelkner**

I cannot comment on that. But really, what we see is customer moving over. There are areas also -- if you go to denial of service attacks for gaming sites, it's much better doing it in the network, filtering valid traffic to the gaming site, when the site is under those attacks, doing that in the network. That's basically security as a service. Then doing it on the premises, filling up the link.

### **Nikki Babatola**

So it really depends on the application that you're moving to the cloud and what you can afford to move to the cloud versus what needs to stay in the infrastructure.

### **Steve Broadhead**

But in terms of cost-saving, on the administration side, a point Rik made, things like patching updates, just general hardware upgrades, are incredibly expensive, not just from the physical CapEx, but the OpEx are massive. So any of us could actually just draw a virtual graph and show the point at which it actually becomes preferable, from a cost perspective, to go into the cloud.

### **Annette Stadler - Markt & Technik**

Can you give us some numbers for how many customers you have for cloud services, for example, in Germany, of how many users and which kinds of services they use?

### **Rik Ferguson**

So from a Trend Micro perspective, in terms of people that are using OfficeScan, I can't give you solid customer numbers because I don't have them in my head. But the numbers I do have in my head give you some idea of the scale of the operation, if you like. So I can tell you that on a daily basis, the Smart Protection Network deals with 29 billion queries and it stops 4 billion threats every day.

And in terms of numbers of customers who are using the Deep Security product, it's a big number and it has some very big names. Some of them I can mention, like the U.S. Military uses it. Some very, very big retailers use it for things like PCI compliance because there are a lot of PCI points that can be hit by host-based intrusion prevention, and file integrity monitoring and log monitoring, which are all extra functions of the product. I can get you solid customer numbers, but I don't have them in my head.

### **Bo Fjelkner**

I cannot comment really on customers, besides official information. And considering the broad range of products, as well, I'm just going to pinpoint two of them. Forensics, for instance, if you have a data bridge, customer calls us and says, "Fly in people," a large bank or whatever. And you can read the number, how many there are, in the data bridge report because the foundation for our data bridge report comes from that work. But it's around 100 per year, or something like that.

When it comes to computing as a service, the offering, we have two official press releases on a real customer. The service was launched in early autumn. But two cases.

### **Nikki Babatola**

Thank you all for your time. And if you have any follow-up questions, please feel free to grab us after this.

