NETEVENTS

EMEA PRESS SPOTLIGHT ON 'THE CLOUD'

First Draft

Debate Session 3 - "For every cloud a silver lining" - addressing the security challenge

Mike Spanbauer

Managing Director, Research, NSS Labs

Panellists:	
Dr Hongwen Zhang	CEO, Wedge Networks
Dominique Assing	Senior Security Consultant, BT France
Derek Granath	Extreme Networks, Senior Director of Product Management

Hello and welcome to debate session three. So the topic today is going to be discussing a bit about cloud security as well as the challenges that enterprises face. So we've assembled a panel of experts that'll comment, as well as provide a bit of a bright lining. So the iron component is of course implying that clouds can indeed be secure and capable.

So, with that, I want to introduce my panel. So here, on this end, we've got Dr Hongwen Zhang from Wedge Networks. Next to him is Derek Granath, who's with Extreme Networks. And beside him is Dominique Assing from BT France.

So a bit about NSS Labs, just quickly. If you're unfamiliar with us, we are a testing security analyst house. So we focus on, in essence, grilling the products and making sure they deliver on the promises. A bit about the markets that we cover.

But what I wanted to also share and set up for the panel here is the fact that cloud security is indeed challenging for many. So in the last 20 years, as I've watched IT and technology evolve, and I think everyone in the room has been exposed to this, studies and concerns around letting go of your data, which is at the core of why the cloud security is challenging, makes people nervous, makes people a bit reticent on production, deployment and evolving to a fully cloud employed model.

So consumption, however, is evolving faster than development. Regulatory, audit, factors that contribute to security policies and models that need to be considered as one looks to and embraces cloud migration.

So factors of consideration. You need to understand the risk and acceptance. Data, who, where and how is it maintained, owned? Incident response or IR, remediation, getting to the root of the breach or an issue in the security models as well as understanding sunset-to-sunrise product adoption, deployment and development.

So the question that I want to pose first to the panel is, as you engage with and discuss with your customers cloud inhibitors, what are you seeing as their biggest concern, their biggest inhibitors today for moving to the cloud from a security perspective? So please, doctor.

Dr Hongwen Zhang - Wedge Networks

Yes. So I'll take this question here. So if you look at it that when the early days of the cloud adoption, security practitioners particularly hear a lot of anxieties from our customers, so this is separation anxiety. And later on, with cloud really being adopted, the whole dynamic changed.

If I look at it that the inhibitors today is really the look at it, we have with cloud adoption, especially with corresponding mobile data usage, we see a lot of invalidation of the traditional security assumptions. And number one is that perimeter is gone and now you have many millions in the cloud, running and where are the boundaries? And you have a lot of mobile devices accessing cloud assets all the time. Where's the boundary? So those are the things that really are customer concerns.

Mike Spanbauer

Thank you. Derek?

Derek Granath - Extreme Networks

I think it's three things, and maybe the first of the three people have overcome. I actually started in the storage networking industry about 12, 13 years ago, and there were storage - they didn't call it the cloud back then, it was outsourced storage services and customers were extremely reluctant to let go of their data. And those storage providers, storage as a service providers were not very successful. I think largely people are now accepting in that the security allows them to safely put that storage or put their data in remote cloud-based data centres.

I think the security of that data is still of concern. Companies are worried about a breach that could cause a loss of intellectual property. And then I think people are still concerned about disaster recovery, although I think a good cloud provider with every good cloud infrastructure, whether private or public, can certainly overcome that as well.

Dominique Assing - BT France

From our point of view, the main [reasons] for which our clients are reluctant to move to our cloud systems is because ground conditions regarding those security requirements are not very often well enforced. For example, everything about access control and so on, within local perimeter of the companies. If you have some products, if you move to clouds, all companies' IT know that in the cloud all these problems will be multiplied at the scale. All problems will be bigger. And because ground conditions, basic questions about security are not correctly enforced right now, going to the cloud and just having more big problems. So that's the main reasons we have encountered with different clients.

Mike Spanbauer

Thank you. So these are indeed the same inhibitors that I've heard in my conversations with enterprises and I'm sure that you've heard echoed throughout the industry. So whether perceived or real, security always comes up in the conversation of where the cloud is hosted or where the data is hosted rather, what type of cloud model that one employs, as well as the management process and policy components that go in the - basically employing a cloud strategy.

So in regards to how each of you have addressed these inhibitors/concerns/perceived issues, I'd like to ask the panel to comment and to provide a bit of perspective in their own words. So please?

Dr Hongwen Zhang

Yes. So with all the moving to the cloud and mobile data accessing the cloud, my company, Wedge Networks, we actually see the cloud is a preferred way of delivering security because the boundaries are disappearing anyway. And so what we provide is a kind of security platform, and we partner with service providers who come to provide the connectivity. We make sure that when you are using your mobile devices, accessing your cloud assets and the path is clean, we try to send data from one place to another place that the path is clean. So from a lot of our teams' point of view, it really is new opportunity for offering a great security services to the end customers.

Derek Granath

So I probably don't even need to say this, but security needs to be a very holistic strategy. It's not just in the switches or in the servers. It's everything from a strategic-level decision about who is allowed to access what kind of data. It requires access controls for mobile devices, network access to control [mac] type function. It requires policies and procedures being programmed through active directory and similar types of databases.

From Extreme Networks, we're part of the plumbing, the infrastructure. So the things that we've actually done play a part in that holistic strategy. And it's the ability to identify users based on mac address and IP address and tie back to active directory and what policy or what assets, IT assets they're allowed to access and not access and

then putting some mechanisms in place through ACLs in the switches themselves. So that's a role that we play. But I don't think any one part of the cloud architecture can be responsible for the enforcement of security.

Dominique Assing

Yes. I totally agree about some security. It's not only a technical point of view. Many problems we have with moving to cloud is more about some convince about some utility, for example, of risk assessment and so on.

We are doing our best to help our customers to be aware about the value of information. Cloud is just putting your information from your companies to somewhere else. And the main problem is very often value of information is not correctly evaluated. So when we are talking about cloud and securities, means paying - buying some different security devices and so on. So there is a cost. And this cost can be only be decided to support it if - only if you have the real value of your assets that you're putting in the clouds, and this means risk analysis and so on. And so we're trying to make people aware that these, with different questions, is very important. So it's not necessarily technical solutions, but it's the basic, before going somewhere for adding more solutions and security.

Mike Spanbauer

Thank you. I'm going to follow this up with a question that we talked about at lunch, which is the architectural shift which each of you have touched upon a piece of it, but I want to come back to it. Would you agree, first, that this indicates a breakage in the asset-centric security model? So we established 15, 20 years ago in IT the security of asset by asset, and in fact that's really what's evolved. It has become more application-centric or driven towards business use case as opposed to trying to isolate and secure element by element in the environment.

Dr Hongwen Zhang

Yes. I think that if you look at it, there are a lot of tried and true security solutions, the typical antivirus, antispam, and nowadays for compliance purposes, PCI [sleeper], those compliance requirement issues, all those things. And if I look at it from the traditional security services function point of view, combined with what is the true spirit of cloud computing, which is elastic computing, right? Security really needs to be handled, as is the question here, really needs to be elastic.

So we are seeing the industry is doing a lot of work, for example the ISDN OpenFlow initiative. And today we hear the cloud Ethernet initiative. This elasticity of security is really needed for a lot of organisations again. Suffice to say that worldwide, and starting to see that the global security breaches cost trillion-dollar damage, we already spend $60 billion each year on security, but still have security issues. We've got to look at it from the different angle, and the cloud provides a tremendous opportunity to do so.

Derek Granath

Yes, again I think it comes back to that holistic policy. Some of those applications don't have security elements in and of themselves. However, senior management from a business standpoint may need to protect who's got access to those applications and who doesn't. [ECI] have a great example of that. So again, in the cloud, whether it's in the cloud or whether it's on the premise, there's still that high-level security strategy that has to be in place first, and then you've got to still look at all of the different elements that - of the infrastructure that provide that security.

Dominique Assing

Right now the security question regarding cloud is very interesting for security industry because very often during the past, we just thinking security like IT people talking about IT problems and so on. Now, if you are considering a business case, of the clouds you have to reorganise the way you see security, the way you are thinking security. It's no more just technical problems. It's more to be sure that what you wanted to do and how to deal with problems. And I think from a business aspect, it's very important that IT people are no more too long talking with just IT people. They have to talk like business people.

Mike Spanbauer

I fully agree. So it's a brokerage between the product lines as well as the IT department. It's a collaborative relationship that have evolved as we've grown more mature in regards to cloud adoption, as the technology has become a bit more comfortable. And I think that there's still work, of course, from a policy definition, from a collaborative relationship. And as the disciplines or silos in traditional IT continue to dissolve, or at least become a little more transparent, isolating each of the distinct technologies that compose the cloud in mass, we can further accelerate because of course security is a layer that runs amongst all as well as out into, well, the providers and beyond. And so it's no trivial single-point solution to overcome.

However, the technology's in place, I think many would argue. And in fact, most of the challenges for adoption stem from that initial relationship and agreement in place. So we have a few minutes that we wanted to actually pose some questions to the audience. And if you've any one that you've got that's just tickling your mind right now, feel free to fire it off, or I'm going to pose one for you. So open mic first?

Okay. So no?

Ambrose McNevin - Datacenter Dynamics

Hi. It's Ambrose McNevin from Datacenter Dynamics. I've heard recently a lot about security over the WAN and one of the emerging issues being the security around data routine. A lot of the CIOs I speak to say they don't want to own data centres and they certainly don't own the network, but what they do want to do is move large files that require security between data centres and geographically diverse locations. So I would say one example being from the UK to India.

One of the issues that seems to be emerging is how secure is that data as it's routing between those two data centres? Where do you guys - is there any progress being made and where do you guys see the actual responsibility for that lying?

Dr Hongwen Zhang

Yes. May I take this question here? It's very interesting that we, our company recently sponsored a university research program, which is related with the data encryption in the cloud. And I think that somehow to provide protection for confidentiality of data, especially when it's residing to who knows where, different countries, and it's very, very important, I consider this is a really very hard area and there are a lot of research that Wedge Networks sponsored.

And I also notice that typical cloud providers, for example, that one knows, Amazon recently announced that the new service offer is really the PKI-based offer, and so what I can see is that there are good trends in the industry to try to resolve this issue. I don't think this issue has been resolved yet.

Mike Spanbauer

In regards to that storage provider that shall remain nameless that went offline or is in the process of their petabytes that they have to get off those discs, so this is a problem that's come up a few times in conversation recently. There's no graceful answer, but it's being looked at by some - by millions.

Did I see another hand?

So with respect to policy recommendations, so all of you talked or touched on this. Best practice, I've seen a number of published best practices, but the - what advice would you offer in regards to pursuing a security model made for this next-gen cloud? It's not as simple as just turning on a new service, defining the security SLA, the SSLA, I guess, or the model to evolve forward, double up encryption or what have you. What would you provide for advice?

Dr Hongwen Zhang

Yes. If you look at the security policies, and there are multiple realms of security policies and, for example, that Mike just mentioned, different kind of maybe encryption. And I think that if you look in the cloud, we see two major trends. One is the policies for really doing digesting and a real situation of awareness of how things are going, which is related with identifying security breach incidents. That's a growing area. And I would see that traditionally in this area the weakness has been to understand truly the application data that flows through the network. And there are a lot of packets and bytes that particularly are very important.

And most importantly we also, which is Wedge Networks really championing this, is have a self-healing network where the policies can be used to really define against real-time attacks. I think this is a growing area which has been - we are seeing tremendous growth there.

Derek Granath

Well the piece of advice that I'll talk about is to the provider of the cloud or to the builder of the cloud. I think most businesses understand the security requirements that they have. But as a cloud provider you also need to understand the security requirements of the customers you're going after. And what I mean is for things like PCI and for HIPAA, it's not only keeping data secure and protecting the access to that data, there are a number of different auditing requirements, reporting requirements that have to be in place and you need network management infrastructure in place to be able to provide that audit.

So it's really, as a cloud provider, public or private, it's understanding your customer and what their requirements are. And it's unique to each different vertical.

Dominique Assing

Well I will have a very different answer to this question. I spent a lot of time about techniques and so on, that's creating a device measure and so on. I'm pretty sure that the best policy we can have should be to be able to correctly communicate with the board, with your board of the customer, and to make a lot of awareness with them to teach them, to learn with them what security is, really what the cost is. And it's not specifically related to cloud systems. It's general. But the cloud isn't just a case, very specific case.

You can define every kind of policy, every kind of security measure, every kind of encryption system and so on. If you're not able to convince the boards that this is the right way to do things, there is no solution. You will have some security measure in the cloud and so on. But at the end, the level of security won't be very good at all, especially regarding the different attacks. We can see now more and more sophisticated.

Mike Spanbauer

That's a great point. Applications were initially designed for scalability, performance or some particular feature, yet security was second, third or fourth on the priority list. So we're addressing, dealing with and remediating these issues now. But first and foremost, prioritisation from the board and ultimately budget are required.

The last question that I'll ask, and this is - it'd be neglectful for me not to mention it, is the emerging promise of capabilities of inserting security technologies within the network, in the end, network function virtualisation, SDN, etc. What do each of you see in regards to your own specialties? A promising technology on the horizon or capability that'll unlock the cloud for this next step, this next phase?

Dr Hongwen Zhang

Yes. So yesterday when I checked into this hotel, the first thing I did, I called the front desk to ask if the tap water is still drinkable. And the reason for that is because I just travelled to a third world country where we have a reseller there. I go to the hotel and we are not to drink the tap water. I think clearly security needs to be in the stage

where when you actually open up the network connectivity and no matter where you get the content, it is clean and secure. That's really the ideal situation. And from that perspective, we see service providers, cloud service providers, ISPs and MSOs are really in a very good position to ensure a clean pipe where we do not have to worry about these kind of breaches any more.

Derek Granath

So keeping the pipes clean is one of the evangelism points that I try and communicate every time I talk about SDN. At least six months ago in the industry, everyone said SDN's going to commoditise the switches. You're going to be able to build an enterprise class network on little netgear switches. And I think you're going to get contaminated water. I think to do SDN right, and centralising control has lots of benefits, but you've got to push the policies down to the switches which are moving water from point A to point B. And those switches have to have big tables that can support access control lists. They've got to have forwarding tables that are big enough to satisfy these million [VNs]. And to keep that water clean, the data forwarding plane has to be robust enough to deal with that.

Dominique Assing

Well, emerging points, from our point of view, what we see regarding our clients is more a switch from a passive defence system to a proactive system. It means we see more and more very often our customers rethinking their defence systems. And now they're trying more and more to put some different layers of defence even in the clouds and within their own perimeters. This is a very big move because this is a kind of methodology we see in the army systems. And there is a very big move from passive defence to active defence. It's not necessarily technological or emerging points, key points, but this is a new way to think the way to protect your system.

Mike Spanbauer

Thank you. So, as you've heard, and I think as many have experienced, enterprise users are like water. They'll find a leak in any security system and exploit it or, whether through accident or intent, expose the dataset. As consultants and technology professionals, it's our job to make certain that the education level rises and that the right policies and all the mechanisms are in place prior.

So with that, gentlemen, I want to wrap things. And unless there's another question from the audience, we will, I think, finish the session. So thank you.

[End]