NETEVENTS

EMEA PRESS AND SP SUMMIT

Draft

Debate VI: Network Security - Revenue for the Telco, Service for the Enterprise

Chaired by: Bernt Ostergaard

Analyst and Service Director, Quocirca

Panellists:

Jan Guldentops	Director, BA Test Labs
Steve Broadhead	Founder & Director, Broadband Testing
Jordi Gascon	Senior Director, Security, CA Technologies

Manek Dubash

So I'd like to welcome to the stage the next debate we're going to talk about. It's funny actually, we've got this far into NetEvents and only now we're talking about security, which is quite rare, really, because usually it dominates everything in these conferences. But yes, next debate, let's talk about security. If the panel and everyone would like to come on down, that'd be great. Come on, move it.

Bernt Ostergaard

All right, thank you. Welcome to the topic that is one of the big ghosts, the invisible partner in this show; security. It is a huge topic so there's no way that we're going to be able to cover it in the time we have. I'm pleased to have a great crew here on the panel side. Basically, what we have is Jordi Gascon, EMEA service security sales for CA. So he's our vendor. We have Steve Broadhead who is our tester. We have Jan Guldentops who is our analyst. So I'll let the panel introduce themselves in a while. But just have a few introductory remarks for this issue.

Clearly the security from a networking perspective is a complicated combination of performance of the network, the apps we're using, the security we're deploying and our internal GRC, and I think governance, risk and compliance is really a key deciding factor here. If I look to the last 10 years of security debates, what's really changed is that we've moved from arcane discussions of security - and I'm sure Jan and Steve and Jordi will get into that arcane discussion as well - but we've actually transitioned to a board room issue, a business security issue, business continuity issue that is using a different language and is opening up the issue.

At Quocirca, we recently conducted a study of how much is actually happening in the European server business. We found that certainly in Germany, France and the UK, a normal commercial server is transacting over 40,000 transactions in a day. So to handle the load and to be efficient, what we see of course is virtualisation and we're seeing cloud adoption. We're also seeing the old Jericho agenda, namely that all devices are potentially hostile. All devices can be compromised. So you're back to, well can I actually control my data and protect that? I'm sure that the panel will have several things to say about that.

The usual discussions of better or worse. I think it's certainly getting better in that we have more specialists in the field and they talk a business language that management actually somehow understand. We have end-to-end perspectives. We're not just looking about the network, the WAN or the datacentre, we're actually looking end to end. We have policy processes. We've gone away from RU, ISO27001 compliant, tick in a box, yes, to how is this actually affecting my business and can I actually defend what I'm doing from [a business] process?

On the bad side, we have specialists. On the Black Hat side. We've lost control of the devices, we've lost control of the applications and we're putting a lot more data onto internet-accessible sources. So one of the things that - the focus I've asked the panel to look at is, how do we control the devices? How do we control the data? Especially, what is the role of encryption? Those of you on the business side who've ever had a presentation from a managed security service provider would have seen these enormous cakes that managed security service providers can bake for you. Frankly, I think it's a hard sell, it's very hard for the companies' buyers to understand what the hell they actually mean. So we are probably seeing a lot of investments that are completely redundant.

Of course the problem is, what is success here? The success at the annual assembly of the company is, nothing happened. That is the greatest success story a security specialist can give his company. But it's a hard sell. One of the other recent studies that we've done is around enterprise apps stores. One way of defending your - both your users and your data by having it in an app store. But what we're seeing, of course, is that that also provides or opens up a lot of possible providers. So the trust issue, do you go with your system-integrated, do you go with your telco, do you go with pure plays, do you go with hard or soft developers? They're all offering these things.

Overall, I think at the moment, the pure plays are winning, the [Iperians] and the [Goods] seem to be cornering this market. But again, that's certainly a discussion that we can take.

So with that, let me turn over to Jordi first to give us your impression of what is the status today?

Jordi Gascon

Security is really big, as you mentioned. For me, I think it's an attitude. For the topic of today, for the revenue for telcos or [answer] for them, this is what they can expect [of] security when the perimeter is [one]. I think it's an important topic. We cannot rely on classical security because you don't control the end-to-end transaction for the [user]. So we have to go further and look into the [unclear] identity as the new perimeters. So you have the identity, you have your mobile, you have your device and you have to [unclear] that [unclear].

So it's a big issue but also in the sense of the telcos and other service providers providing security, we believe that can be done. [We don't hear as much] when, as a service, it's a reality today and the technology allows that as well. If you say okay, well we are giving control to the service providers or the telcos, I always put the same example of the guard in the [van] that is a third party employee and has a gun and is inside the branch office. So we need to learn also to give some control, obviously, inside a framework. But that will allow a specialist to take, also, on the security of the organisations.

Bernt Ostergaard

Okay, so here we have the reassuring view. I'm sure that Steve will talk about security as a child with matches.

Steve Broadhead

We quite like that reference [down here], yeah. So I'm not actually just a security guy, I test everything in the infrastructure. So one of my main roles is actually where you put security alongside other devices like WAN optimisation devices, et cetera, et cetera. Within the confines of a LAN and a private WAN then the talk of perimeters is relatively straightforward. But if you're moving stuff out into public-private class, so you've got several different layers of security and several different perimeters and then you've got data passing between those, that for me is a kind of a critical area to look at here. Not just on the security perspective but how we combine that.

So for example, there's an order of things. If you want to optimise traffic, if you secure it before you optimise it, it cannot be optimise because it can't see what it is to optimise it. So that's simple in a one-box scenario, optimise the traffic then secure it. But what if you've got several layers that that data's passing through? Do you keep on encrypting in, unencrypting it, optimise it, encrypt it? It's fundamental, it doesn't work, absolutely.

Bernt Ostergaard

So moving from the tester's perspective to the analyst's perspective. Jan, what is your take on security right now?

Jan Guldentops

Well I'm not really that much of an analyst, I just look at things and see what's happening. It's - there's three things I would like to say. The first thing is a service announcement. I know - I don't know if you guys have noticed but there is a serious Bash bug out. So Bash is the shell in every UNIX system, including those MacBooks you see here and there. It basically is a route exploit that is remote executable. So although we have bad Wi-Fi here, I would be updating my MacBook straight away. If you want more details, I've put it on my twitter account. So that's the first thing.

The second thing is, I've been doing this for 20 years and there are two constants. First of all, nothing ever changes expect more [slow]. We have more bandwidth, we have more CPU power but next to that we're still making the same stupid mistakes. If it's being made by the telco, by the supplier or by the end user, we're still doing it. Secondly of all, there's only one real security product you should know. That product is common sense. We have this attitude of, oh, let's give it to the security consultant or the telco or the managed security supplier or whoever. As long as I, as a CEO, don't have to think about it.

Well that's wrong, the CEO should understand what security is. One of the schematics you should look at is the circle of [damning]. The quality [client] management thing, the circle with plan, do, check, act. That's what you should do if you do security. Then you should start looking at software and solutions and other stuff.

Bernt Ostergaard

Thank you, so let me take just a recent case that most of you may be aware of, and I want to ask the members of the panel what their advice to this company would be. So the company's Home Depot, large US retailer, they had an unfortunate incident where 56 million credit card details were stolen from them. It turns out, they hadn't updated their virus protection since 2007. They did not consistently monitor their networks for signs of attack. They failed to properly audit eventually hacked payment terminals.

So is Home Depot an exception and what's your advice to these types of customers? I'll start with Jan since he seems to be most agitated.

Jan Guldentops

No, it's not an exception, it's the rule. What I noticed over the years is the companies that are most arrogant about their security have the biggest holes behind the curtains. In the Netherlands, and I forgot the name, they had the CA, Certificate Authority, which - sorry? DigiNotar, thank you very much. Which basically got hacked because they were using trivial passwords in the field of 123456 for their infrastructure. They had public accessible databases.

It's the rule; people make stupid mistakes. One of the things I always try to do is, if you talk to somebody about security, is the number 1 rule is keep it simple. What Home Depot should have done was encrypted their databases with their keys - with their credit card numbers. That would have solved quite a lot. All the other problems would have been less [unclear].

Bernt Ostergaard

Steve, what would your advice be to a company like that?

Steve Broadhead

Keep your antivirus up to date, absolutely.

Bernt Ostergaard

So we're back to the issue we've talked about various other discussions and technology, not just this NetEvents but others, and that is how do you cope with the human element, the human failure element? So since probably the early '90s, I've been in discussions about automation of absolutely everything. Cut out the human error. Yet we're still here in 2014 and there's still far more human error than automation. So how do you get to the point - and this will be one for Jordi - how do you get to the point where you actually force the updates on everyone so they have to be in a situation where they haven't updated for seven years? How do we get to that point?

Jordi Gascon

Okay, first I will say that is something called due diligence. So they are not doing...

Steve Broadhead

Common sense as a service.

Jordi Gascon

Common sense, exactly. I have to say that in general terms, the business doesn't like security. They need security, which is a different things. But they have to have security to run the business. Today, all businesses are based on software, it's IT driven. That's a fact. Even the most classical [unclear] business needs software, so need security. What we do, from the vendors' perspective, is try to minimise the risk, to negate the risks. As you say, it's about insiders, it's about misconfigurations, it's about mistakes. So you need to [perfect] the systems also, of the insiders, people - privileged people because you had administrators and it's a bad design of the system. You have root share with several people. So there is no accountability.

So you need to manage this and track all the actions, audit the actions and prevent the actions. There is software to do that. I have to say that fortunately I visit a lot of customers and security [person on] the top and I wouldn't say that [these are wrong]. It's true that it's very difficult to keep the rhythm of updates of the systems and the

[back], so it's a race. So probably the point here is that you need to think in a different way. It's trying to protect the resource and the means of accessing the resource. Even for unknown risks.

If you protect the data, you protect the resources, it doesn't matter if you use Bash or a different shell or other script or whatever you use. I think we provide this technology today.

Bernt Ostergaard

So let's just talk about...

Jordi Gascon

I'm not trying to [unclear] by the way, but...

Jan Guldentops

One of the things that always bothers me is people have the wrong premises. It's not, you should not be hacked or are you hacked, it's when will you be hacked? Everybody will have a security problem sooner or later. It's not a real disgrace. The disgrace is what you do with it. Technology like security and incident and event management are completely - are practically unknown for a lot of good IT guys. Well it's standard common sense. I monitor my devices, I see what alerts they give and I try to make sense out of it.

But it's all - it's not only technology, it's also having the common sense of looking at that and preparing for that and reacting in the right way when you have a security problem. Most companies that have a security problem put their head in the sand, they try to keep quiet and they try to patch it as quickly as possible. That's the wrong attitude. You need to document, you need to approach it. You need to be open about it.

Bernt Ostergaard

So it's like Bob Dylan said, everybody must get stoned. Right, okay. Let me ask you, what in your point - in your perspective, where does security breakdowns really hurt? We hear about banks - we used to hear if a bank was down for three days, it would close. Things don't stop working just because you've been hacked. Companies usually survive this. But where does it really hurt? Both on the individual level and on the company levels? Jordi? Oh, we'll have Steve first. We'll let Steve go first.

Steve Broadhead

I was just going to say, that no, there is a [pain] every time something like that happens, in terms of dollar cost. It might not actually bankrupt a company. But we just mentioned very early on a breakfast about if your house gets burgled, you compromised for the rest of your life. So there's also that issue which is basically, if you think you've got a perfect security strategy in place and then something happens, which it will, then the natural thing is for humans to actually panic and think I must change everything, as opposed to just looking - stepping back and saying, well which little part of my strategy didn't actually work then?

I think that's the biggest problem with any issue is, people panic about it rather than actually just looking at what they should do on a step-by-step basis.

Jan Guldentops

The usual reaction if they had a security problem is lock down everything. Stop working. But the trick is also, there, it's a bit common sense. You should be - it depends a little on industry. There are industries where there's really a problem. Talking about the wireless denial of service attack I talked about earlier that resulted in the [death] of around $11 million of equipment. That almost let the company go belly-up, which I'm not going to talk about who it was.

Steve Broadhead

I was just going to add, actually that wireless, contrary to most popular belief, is actually the most secure form of data transport because you can't get onto it in the first place.

Jordi Gascon

Okay. I have seen much more pain in organisations trying to solve security incidents than the damage from the incident itself. So I agree on that point. I believe that we are - we have organisations that are well prepared for responding to a security incident. The problem here is that they don't know what has happened. That's the real pain. Are you able to track that? What was the initial state of your servers? Can you [unclear] really happened? Then you cannot fix it. If you don't know, that's the worst thing.

We were talking about this morning, it's organisations saying, no, no, I didn't have any security incidents. Well, you don't know, which is even much more scary.

Bernt Ostergaard

Because that gest to the issue of, if we're all hacked and if all our credit card details have already been stolen because we've logged them somewhere on the internet and it's been hacked. So we're all breached. What's good enough security? For example, take the internet of things, huge gorilla out there, what is good enough security? Jordi?

Jordi Gascon

Well that's a quick answer for that one; it depends on the risk that the organisation wants to have.

Bernt Ostergaard

So a GRC process?

Jordi Gascon

Yeah, you have a point where it doesn't make any sense to put much more countermeasures because you are not saving anything. I'm talking not about just cost or this money business but also reputation. So with banks, the company doesn't want to be in the news, they will provide a good set of measures of security. [Multiple speakers].

Jan Guldentops

The question is, is there such a thing as bad publicity for some of these guys?

Bernt Ostergaard

Yes.

Jan Guldentops

No, the trick is, you really need to be able to fix that. To really address what's happening. One of the things I saw, which is one of the biggest problems, is you're never going to be - if you don't have integrity check systems, like host based DDS and intrusion detections systems in your organisation, you're never sure you're clean any more. Belgacom, big Belgian telco, is still not sure that their BRICS network and the rest of their infrastructure is attacker free, which is basically paralysing part of the organisation. So I agree with you on that one.

Steve Broadhead

You are allowed to agree occasionally. So to me it's not just a case of, what level of security do we go for, but how you actually manage whatever security you've already got in place. So again, if you go back to a performance perspective, if you're basically controlling WAN applications across the WAN cloud, whatever, you actually have application monitoring devices so you know exactly what bandwidth is being used, what applications are being used at whatever time, by who, where, why, when. But I don't see that kind of monitoring happening in security. That's exactly what we're talking about here.

There should be someone who's looking down from above on all the elements of security in the company to make sure they're all functioning properly, up to date, et cetera. I think that's critical.

Bernt Ostergaard

So we basically agree that what drives or motivates the consumer is convenience and they will take a risk because it's convenient. But what should motivate a company would be consistent monitoring and auditing.

Okay, let's move - I also want to have time for questions. But very quickly at the end here, what is the role of the managed service provider? Not just the telcos, it could be system integrators. What is the managed security service forte really, in this situation? Jan? Oh, Steve, yep.

Steve Broadhead

I think it's simply to do with selling the service to the right type of company. So if you look at the small medium businesses, which is a mere 93% of IT spend in the world, those are the guys who can't do it for themselves. So they - it's not like a responsibly, it's a fantastic business opportunity for any kind of managed service provider to target those guys and give them a service at a price that is good for the company, obviously revenue for them, but also do it properly. Because one of the other issues with a lot of SMB services and sales is it's seen as the poor man's kind of thing; we're not going to make as much revenue out of it, et cetera. So it's like a second-rate offering.

In security, obviously, that cannot be. One person's security's as important as 7 billion people's security. Likewise companies. So I think the SMB market would be the ideal match for this, so long as they give them a proper service.

Jordi Gascon

Sorry for that, but I will introduce another topic. Because it's related to that one. It's about the application [economy]. So everybody now uses applications to interact with organisations, with business applications. This was mentioned in the previous panel as well, insurance companies but also banks. So everybody has [unclear] so organisations, they need to manage millions of identities. So how do you set up and [infrastructure] [unclear] by yourself to do that? because it's not just managing employees, managing [unclear] managing vendors' identities, now it's the whole population of a country or Europe that needs to be managed and you cannot do that, you simply cannot do that.

So they will need to go there, even the biggest companies are having problems to manage that.

Bernt Ostergaard

What's your perspective, Jan?

Jan Guldentops

In the end, it's all outsourcing or insourcing. It's the balance with every service you do as a company. Is it better and cheaper and more efficient to outsource it or is it better to get your own staff. So - and security isn't different in that field. Of course there is trust, if you hire a security guard in your bank, you don't want them to be overweight and 73, if you want some security.

Bernt Ostergaard

Ageist.

Jan Guldentops

But in the end, it's all down to efficiency and getting the right knowledge in house. Just being able to make it cheaper in operational cost.

Steve Broadhead

Yeah, just to step in on that. It's like people seem to think of security as being different from any other. So oh yeah, I'll happily outsource this, this and this but security, no way. Well what you're saying there is, I will happily outsource things, and I don't actually trust the outsourcing guys but I see that as a lower risk than security, which is nonsense. You either trust to outsource or you don't. It doesn't matter whether it's security or not.

Bernt Ostergaard

So with that, I'd like to open up the floor for questions and comments. Because this issue is just huge so there might be some comments from the floor. Is there a mic anywhere? There's a question down here.

Audience Q&A

Thierry Outrebon, InformatiqueNews

Thierry Outrebon, InformatiqueNews. All the first applications on [SDN] are focusing on security. So does it change something?

Bernt Ostergaard

I'm not quite - what was the question?

From the floor

So the first applications on [unclear] and SDN are focusing on security, HP and VMware are launching applications with all [it shows] is it's the main solution to bring new layers of security.

Bernt Ostergaard

Let's start with the vendor. What are you doing in that space?

Jordi Gascon

Well we are investing heavily and we do more than security. We do [unclear], we do monitoring, cloud monitoring. But security is one of our biggest investments. I already talked about that at the beginning, it's about the need of security. So you cannot put a business application available to the world without security. So it's something really needed. This perimeter that has [been gone] needs a different approach to security in different layers and different strategies. That's [greenfield] for us for developing new security solutions as well.

We were talking about bring your own device, bring your application, bring your own identity. We are talking about [social volume] so [unclear]. So a lot of security needs coming that we need to solve. It's a business need.

Jan Guldentops

It's going to be work for the security guys for the coming few decades. So it's a good gamble to study that.

Steve Broadhead

Yeah, I was just going to say [unclear], it's an ongoing thing. So for me, there's no actual finished product there for me to actually look at and say, that works, or it doesn't.

Jan Guldentops

Well it's one of the things. A lot of people put virtualisation as something magical. It doesn't change the premises. If you do it in SDN or you do it in a virtual machine or you do it in VMware, the basic - hold on Steve - paradigm is the same.

Steve Broadhead

I think, so - if I just say, yeah, so one thing we discussed this morning which is relevant is if everything's in VMs, virtual machines, that - you don't automatically firewall between VMs, you can actually inject attacks from the other, and we've done it as part of the testing. So just because something's virtualised doesn't mean it's secure, anything but.

Jan Guldentops

It's one of the illusions.

Jordi Gascon

[Unclear] it's even worse. Because you have a [new] layer, which is you have the administrators of the operating system and they have [your passwords]. Because they are very [powerful]. At the advice of administrator, I remember a company, a pharmaceutical company and they laid off one of the administrators and from the [unclear] he deleted and misconfigured 200 [unclear]. So it's even worse. So you have another layer to take in account. It's the private usage managing the utilisation.

Jan Guldentops

It's basically one of the hidden time bombs under everything as cloud infrastructure. Because everything is built around x86 hardware infrastructure. Now if there's one thing in x86, it's shared memory. So the only thing between two virtual machines' memory is software. We all know how well built that usually is.

Bernt Ostergaard

I think there is an additional aspect that's really important here. We've talked about the human error as a central thing and the lack of common sense very often in these situations. I think another issue really is the organisational structure. Both in the companies - who is actually responsible for security? Also on a telco side, telco NOCs don't work with telco SOCs. So we do have an organisational challenge.

But I'm getting the sign here that we have to sign off. So basically I want to thank you for the session and of course discussion goes on. So hopefully much more to be learnt, thank you.

Manek Dubash

Okay, thanks Bernt and thanks to the security mavens.

[End]