Thought Leadership Discussion Webtorials

Certes: Who’s Next in the Hacking Headlines?

Lessons Learned from the Data Breach Epidemic

Recorded January 16, 2015
Discussion Transcript

Adam Boone
Certes Networks, Chief Marketing Officer

Larry Hettick
Webtorials®, Editorial Director and Senior Research Fellow

Patte Johnson: Welcome to our Webtorials podcast. Today, our analyst, Larry Hettick, will be speaking with Adam Boone, the Chief Marketing Officer of Certes Networks. The title of our podcast today is, “Who’s next in the hacking headlines? Lessons learned from the data breach epidemic.” Larry, I’ll turn it over to you.

Larry Hettick: Thanks, Patte, and thanks, Adam, for joining us today. We can start with an easy question. Can you tell us a little bit about yourself and your company?

Adam Boone: Certainly. Thanks a lot, Larry, and glad to be here. Certes Networks has been around for about 15 years, and we make products that secure an enterprise’s data whenever it moves over any type of network or network environment. Our products are called CryptoFlows, and you can think of them as super-secure, very flexible, application-aware types of VPNs.

So, a CryptoFlow, for example, could protect data all the way from your application server to, really, any endpoint over any network. It does that with a simple point-and-click. We’ve shipped thousands of these products to customers in, 70 countries around the world. We’re doing things like protecting credit card data, and consumer data; healthcare information; financial transactions; sensitive, top secret records; and much more. And in fact, I’m willing to bet that most people listening to us right now are carrying a credit card in their wallet that is protected by our products.

I myself have been in technology, and especially in networking and telecom, for a couple of decades. I’ve spent about the last decade in networking and also in IT security. For about three years I led a team of white hat hackers, and we did penetration testing for enterprises and service providers, including a number of companies in the Fortune 500. So, you know, I've seen first-hand the state of IT security, and the IT security architecture as it exists in companies around the world.

As far as Certes goes, one thing I'm really proud to say is that we have a perfect track record. In the 15 years that Certes has been selling its products, with thousands of deployments, not a single one of our customers has ever been hacked on our watch. Not one single hack. We're very proud of that track record.

Larry Hettick: Well, congratulations. That's a very notable accomplishment. And it must be a busy time in IT security these days, with widespread hacking and data breaches taking place, such as at Target, and Home Depot, and Sony. We've certainly heard a lot about that, the last few days. Many others have brought a lot of attention on security. But why is this all happening now?

Adam Boone: Yes. It's a good question, Larry. And I think, in a way, that we've all become victims of our own IT success, if you will. You know, over the past 20 years or so, the IT industry has been great – done an amazing job of helping enterprises to digitize sensitive information, and then use it and share it in new and valuable ways.

For example, I'm talking about healthcare data; financial transactions; credit card data; you know, consumer information. Rewind to the last century, and all that stuff was on paper. It was sitting, safely filed away in someone's filing cabinet, under lock and key.

Fast-forward to today, and all this stuff is digitized. We've digitized almost everything. We've made it really easy for you to store these sensitive pieces of data out on the network, or in the cloud, or process them with applications that are on a server attached to your network. And, perhaps most importantly, you can now share them very easily with your colleagues, or your partners, or what have you. And these bring you all kinds of amazing advantages, right? You have efficiency. You have increased the speed of your transactions. You're basically able to get a lot more work done, a lot faster.

But there's the dark side. And having this information digitized means it also can be accessed by remote attackers or unauthorized insiders. Easy sharing means easy sharing with anybody, good or bad. So, maybe, you know, ten years ago the typical hackers were basically committing vandalism, right? I mean, that's what hacking was back then. It was putting graffiti on your website, or maybe disrupting your e-commerce server for a couple of hours. And it might have been embarrassing and annoying but it wasn't mission critical. It was a relatively minor impact on your business as a whole.

That's completely changed. Now, a modestly skilled hacker can access pretty much anything. The mission-critical data that, drives your enterprise, and they can hold that hostage or use it for identify theft, or sell it on the black market. There is now this tremendous financial incentive for hackers today.

And so, that's why I think this is happening now. We're seeing a perfect storm. And that's why we're seeing this explosion of hacking. These two trends are coming together. You've got this digitization of sensitive data, and that's reached critical mass. But it's also now very profitable to spend your time hacking, and probing the enterprise defenses, and trying to get your hands on that data. That's why I think this is happening now, Larry.

Larry Hettick: It all sounds pretty dire to me. Do you think we'll see the same sort of hacks continuing this year, into 2015?

Adam Boone: Yes. I'm afraid we have not seen the end of it, and in fact we may just be in the beginning stages. I think we'll see these kinds of hacks and many more. The bottom line is, the incentive is not going away. There is a market for this data that these hackers are getting, and no one's going to be shutting that market down any time soon, if they ever do.

We're also seeing this sort of evolution in the type of information that's being targeted. With Home Depot and Target and some of the other hacks, the hackers got credit card numbers. And that was their main focus, and that's the information that they were stealing and selling. But with Sony, they actually went after the actual product of the company—movies, and the information that was driving daily business operations. So, it's really going after the lifeblood now of these enterprises—the very products that they sell, and their operations to sell them.

Larry Hettick: So, the impact is really changing for the victims of hacking as well.

Adam Boone: Absolutely. Absolutely. The damage is no longer isolated to some small system, or your website, or a minor supporting application. These hackers are now going after the mission-critical applications that are really at the core of potentially billions of dollars of revenue for these companies, like Sony. And then, of course, there's also the question of who pays to clean up after a data breach. With credit card replacement, and identity theft protection, and fraud costs and damage to your company's valuation and other impacts, the cost of cleaning up after breaches is really swelling into the billions.

Larry Hettick: So, who pays for all that? Who's going to pay for all those cleanup costs now that's changing?

Adam Boone: Yes. It's a good question, and in fact there are some things going on right now that are changing where the buck stops with these breaches. Take the typical credit card breaches. It's often the credit card-issuing banks or financial organizations that are footing the bill. They're stuck with reissuing cards; covering fraudulent charges; doing account monitoring activities and the other types of cleanup tasks. You know, the company that was breached may have the responsibility for notifying consumers of the breach itself, and we're certainly seeing discussions around changing those practices in industry at large. But, right now, as these costs are swelling into the billions of dollars for cleaning up after these hacks, where we're starting to see some real changes in where that cost is going to fall.

Take the example of credit card breaches. A judge in the US recently issued a ruling that clears the way for credit card-issuing banks to sue a breached enterprise, and sue them and accuse them of negligence in their security architecture. That could be huge. That could be a real game-changer in how all this plays out.

Let's say I ran a department store chain. And before, if my systems were hacked and a couple of million credit cards were stolen, the ones who really had to clean that up were the banks who issued the cards. They would have to reissue the cards and cover the fraud charges, et cetera, et cetera. And I've seen statistics that say that one stolen credit card number will cost the card-issuing bank $20 to reissue that card, and then much more beyond that if there is fraud or some other issue that requires additional attention. So, what that means is that just one of the breaches we've seen in the past year could cost the banks more than $0.5 billion just in card reissuing costs alone. Now, that's a big price tag.

So, what's happened is, the banks have taken a look at that, and in one of the cases they've filed suit against one of the recently-breached retailers, and they accused that retailer of having inadequate security architecture or following practices that were inadequate—essentially, accusing them of negligence in their security architecture. Now, I'm not speaking to that specific case, because we don't know if there was negligence involved. But allowing this to go through, a judge agreed to let that bank suit move forward, suing that retailer.

So, what's that mean? In the big picture, it means that you could be held liable if you had an inadequate security architecture and did not follow the reasonable security practices. It means banks could now look to hit you, as the enterprise, to cover hundreds of millions of dollars in costs that they've been bearing before.

Larry Hettick: So, that's a pretty scary prospect if you're running IT security. That mistake could kind of put you on the receiving end of a massive lawsuit. What should IT security professionals be doing in response to all these developments, particularly the liabilities and so forth?

Adam Boone: Yes. Yes. Absolutely. Step number one is just to make sure that the people in the C-Suite—the top management and executives who are controlling budgets—make sure they're paying attention. Make sure that they are budgeting for the improvements and the upgrades that you really need to protect your enterprise.

You know, IT security, frankly, in the past has often been viewed as a kind of a nuisance. It's something that may get in the way of the cool IT projects that you want to do to improve your enterprise operations. But that's a really dangerous and a really old-fashioned point of view. IT security is not a nice-to-have. It's not something where you can try to get away with doing the bare minimum. It should be viewed as a fundamental, mission-critical function, and doing it wrong can really cost you your business. I personally think it's criminal how so many IT security teams are understaffed, and how they're underfunded.

But the good news is I think you've probably got your executives' attention. I think they're probably concerned about their security architectures. And if you think they're not, then slap a copy of the *Wall Street Journal* or *USA Today* in front of them. Because this is playing out in the headlines. Senior executives are losing their jobs over these data security practices.

And what we've seen in recent reports is that IT security spending is now the number one area of IT budgeting worldwide in enterprises for 2015. To look at it another way, if you're not budgeting improvements for your IT security in 2015, then I sure hope you addressed it in previous years, and that you're confident that your security architecture is as modern as the applications that you're using.

Larry Hettick: It's pretty clear that we need to invest. But where should enterprises be investing? What needs to improve in their architectures to counter these attacks?

Adam Boone: Yes. It's a good question, and one that we've been engaging in with a lot of our customers. Based on what we're seeing there, there are a couple of projects that we view as the low-hanging fruit and that our customers are seeing a very high return on investment when they address them.

Step number one is improving the security of data traffic. So, I mentioned earlier that there are lots of these networked applications that are now carrying this essential corporate data, and much of it is extremely sensitive. And part of the issue there is, more and more of this traffic is leaving the enterprise perimeter. It's going, beyond the firewall, or the traditional secure perimeter of the enterprise.

And therein lies the problem. It's the fact that the systems we use—the VPNs and encryption tools that are supposed to protect that data, okay, and keep it segregated; keep it safe from the hackers—those tools were invented and perfected last century. We're talking about tools that are 20 years old now. And they're tied to gateways, or firewalls, or routers. And they're often very static and siloed, and frankly hard to use, hard to configure, and fragmented – that you may need five or six or seven different systems to control the full path of a dataflow.

Or they may be reliant on things like SSL security that's embedded in a single application. And so you're at the mercy of that application developer. You don't know what kind of open source components they may have included in that application; you're not in direct control of the security policies or the encryption algorithms, et cetera, et cetera. So, you've got a lot of issues around this fragmentation of security in this sort of environment.

Every once in a while you'll see either articles or presentations from analysts that say the firewall is dead. I don't think that's accurate. I don't subscribe to that. I think there will always be a need for firewalls, and firewalls are really a foundational or fundamental part of the architecture.

But firewalls are not the best tool for protecting your data traffic. And that's especially true if that data traffic is going outside the enterprise. Think of it this way: firewalls are focused on keeping the bad guys out. But protecting data traffic leaving the enterprise is about actually extending your data security to follow the data. It's proactive. It's not about keeping bad guys out; it's about protecting your data proactively.

I'll use a simple analogy: it's like the difference between having a castle and a suit of armor. You need a strong castle wall to keep out the attacking hordes of invaders, right? But if you and your knights are out running around outside, then a castle wall doesn't do anything at all to protect you. You need suits of armor. You need suits of armor to protect you while you're out there, mobile, beyond the castle wall. And those suits of armor are like VPNs.

I'm sorry if {laughter} that analogy seems kind of silly. I probably watch too much *Game of Thrones*. But my overall point is that the – protecting our data traffic is really fragmented. We recently sponsored a survey conducted by Spiceworks, and it asked IT managers around the world how they're protecting their sensitive data traffic. And more than 75% of them replied that they're forced to use two or more forms of encryption for each dataflow. And around a third are having to use three or more types of encryption for a single dataflow. I need to touch three different systems in order to secure traffic for a single application to a single user or site? that's seriously broken.

Larry Hettick: How are you advising enterprises to protect their data traffic?

Adam Boone: From our point of view, and what our customers have been effectively deploying, is this idea of unifying your protection of data traffic and eliminating that fragmentation I was describing. So, in practical terms, what's that mean? It means, you know, instead of using IPsec tunnels for some data traffic, and then VPNs for other data traffic and other segments of the data path, and then still other methods like SSL, you instead find a way to simplify and rationalize that into a single flow that can manage those end-to-end.

And that's what we've done. That's what our products do. I was describing earlier, our CryptoFlow Solutions. What we do is deploy these encryptor products in the enterprises, and that allows them to have a single interface to define and control these CryptoFlows that go end-to-end, from an application all the way to whatever endpoint they want to protect to. It might be a smartphone. Might be a tablet. Might be a data center site. Might be an enterprise remote office. And then our system protects that traffic end-to-end, automatically. And this includes internal networks, by the way. And that really is a whole other area of security architecture that needs a lot of attention.

Larry Hettick: So, what's the problem with security architecture today for internal networks?

Adam Boone: Local area networks traditionally are assumed to be secure. You consider that to be the, quote-unquote, trusted network. And unfortunately, that's just a hopelessly old-fashioned idea. In almost every single one of the high-profile breaches we've seen over the past two years, the internal traffic and lack of security controls on the internal traffic has been a major, major factor.

For example, a common tool used by enterprises to manage their traffic on internal networks are VLANs, or virtual local area networking – networks. And that's used for segmenting traffic internally. But people often make the mistake of thinking that VLANs are secure. They're really not. They simply are designed to logically segment traffic.

It's trivially easy for hackers to hop from VLAN to VLAN, to move from one part of the network that may not be particularly sensitive, into another part that is very sensitive, carrying sensitive data. It's trivially easily for them to make those hops.

The bottom line here is that, in case after case, we've seen hackers who get access through the firewall, and then they have free rein to go anywhere at all in the enterprise. So, even the most sensitive applications are not protected from an insider or a hacker who gains that access.

And the only answer is to assume that that internal network is untrusted. You have to assume that either a malicious insider, or an external party, or some type of malware, is going to compromise that internal network. By the way, we're not the only ones who are seeing this or saying this. Gartner, Forrester, and other top technology analyst firms have been advocating this position for years. They say, look, you need to accept the fact that, really, no network can be trusted today, and that includes your internal network.

And our own customers – I know probably the ones that I consider to be the most secure, have been operating this way for years. They set up internal encryption of traffic on their internal networks, just like they would as if it were going externally, outside the firewall.

So, we call that cryptographic segmentation. And the idea there is that you're designating a sensitive application, and you use encryption to encrypt the traffic for that application everywhere: outside the enterprise, inside the enterprise. And you use that encryption to isolate the servers and the endpoints, and really create their own cryptographically protected segments.

The challenge with this approach, of course, is that the typical gear that is used for encryption for network and security vendors—you know, I'm talking about your garden-variety routers and firewalls—those systems are absolutely crushed by the encryption processing burden. And we've seen lots of statistics, and in fact it's widely documented that these firewalls and such – their throughput will be whacked by 75% or more when you have to turn on real-time encryption processing on them.

So, that forces a really dangerous tradeoff. I can be safe; but then I bring my network and applications to their knees. You know, I can be safe or fast, but not both. It's ridiculous, honestly. You think about it. It's like you just bought this awesome sports car, right? And the sports car can go 160 miles an hour. But if you put on your seatbelt, then it can only go 40 miles an hour. I can go fast, or I can be safe; but I can't be safe and fast at the same time.

And it would be comical if it weren't such a big part of this whole cybersecurity problem today. So, it really is certain vendors of networking and firewalls who are forcing this tradeoff between being safe and being fast. And in my book, those vendors bear a huge part of the responsibility for this hacking epidemic that's going on around the world.

Larry Hettick: So, what's the answer to that tradeoff that you talked about?

Adam Boone: The answer is not – frankly, it's not to rely on systems that were created for some other purpose. don't expect a system that was created to do routing or firewalling, to also be able to protect your data traffic in real time. You know, your firewall, your router, is focused on performing a different function, and it's not necessarily related to encrypting data traffic. I always say, let the routers route; let the switches switch; let the firewalls keep the bad guys out. Protection of your data traffic is too important to be a hobby.

And so, our customers rely on us to be an independent data traffic security solution. And that's exactly what our products do. We use the strongest standards-based encryption to secure traffic all the way from the application server to the endpoints and the users accessing it. We have one pane of glass that allows you to set up and monitor that protection from end to end, and can literally set up a security policy that protects single applications traffic for all the users, for example. You could have various policies for all your applications, with different access rights. You could mix and match for different users, and have these – the policies automatically be assigned and enforced. And it's all point-and-click, and end-to-end, so that you can be insured that your sensitive application traffic is protected both inside and outside the enterprise.

Specific to the tradeoff question, our CryptoFlows are fully independent of the network devices. They're independent of the firewalls and the applications. So, there's no performance hit there. There is no configuration change required. In fact, the network devices and the firewalls don't even know that our encryption is functioning. And we're also compatible with any of the standards-based networks out there.

So, that eliminates the tradeoff, right? You can have top-performing networks and top-performing applications without trading off the security and putting the data at risk. You can drive your sports car really fast, and wear your seatbelt at the same time. So, you can be fast and safe.

Larry Hettick: So, what next – what are you guys going to do next? With this new focus on IT security in the enterprises, what sorts of new products are you planning to introduce to evolve the security architecture?

Adam Boone: Yes. So, we, in fact, just introduced a new version of our CryptoFlow solution, and it extends your security all the way to smartphones. With the first release, we're supporting the iOS-based endpoint devices: so, your iPhones, your Apple devices, your iPads, et cetera. And this means you can now extend that same application security architecture I was describing, out to these endpoint devices and mobile devices that your employees are using. And by the way, you can also extend that into the cloud. You can extend it into your data center. You can have these group VPNs with a very straightforward, simple policy enforcement and keying, to touch all these different devices and their dataflows.

Now, coming up next, we're going to be releasing versions of that for Android and Windows Mobile. And we're also going to be having a special focus on providing end-to-end encryption for ruggedized handhelds; so, the segment of the enterprises that used ruggedized devices for various types of functions. And we've just had a huge response to this development from our customers and our resellers.

Now, just instead of having a single VPN server that's sitting off in some silo somewhere, you have true end-to-end encryption, all the way from application servers all the way out to these end devices. And it's extremely fluid and application-aware. It follows your users no matter where they go. And it really provides this end-to-end security all the way into the cloud, if that's where the data is destined to go.

And we're compatible with mobile device management solutions and enterprise mobility management solutions, and in fact a number of the MDM vendors that we're working with we're able to allow them to seamlessly and, really, painlessly integrate their solution into the rest of the security architecture. So, it's a very powerful added benefit.

We've also just released an enhanced version of what we call CryptoFlow cloud, and that's aimed at cloud and virtual environments. So, our solution now protects data traffic even in virtual environments like software-defined networking or network function virtualization. And we're the encryption solution of choice for the ecosystems of six different NFV and SDN vendors out there right now.

So, Larry, it's really going to be this continued evolution of how we protect sensitive data traffic. And frankly, we're really excited to see what's happening out in the industry, and this renewed emphasis on IT security as the IT security architecture is evolving. We're really looking forward to maintaining our perfect track record and never having a customer hacked on our watch.

Larry Hettick: Well, great. Thanks very much for your comments. Been very insightful, and it looks like it's going to continue being interesting time ahead of us. And with that, Patte, I'll turn it back over to you.

Patte Johnson: Thank you, Adam and Larry. It's great to know that effective security solutions are available. And we hope that the Webtorials audience will add questions and comments to this informative podcast. Just go to the Webtorials website and let us know what you're thinking, and continue the discussion. Thanks for joining us today. We appreciate it.

THE END

Webtorials® is the premier Internet site for IT-related education and resource-sharing. We provide an interactive communications platform that unites all members of the broadband networking and IT ecosystem: enterprise and small/medium-size business (SMB) IT professionals, solutions companies, service providers, analysts, consultants and press. Here, they all share their favorite documents, exchange problem-solving tips and participate in community discussions.

For over 15 years, Webtorials has provided its worldwide community of networking and IT professionals with a wide range of resources, including **White Papers**, **TechNotes™**, **Thought Leadership** , and **Research Reports**.

For editorial questions and concerns, please contact **Steven Taylor**.

For questions concerning marketing and highlighting your products on Webtorials, please contact **Sales@Webtorials.com**.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward-looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.webtorials.com

Division Cofounders:
Jim Metzler
Steven Taylor

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.