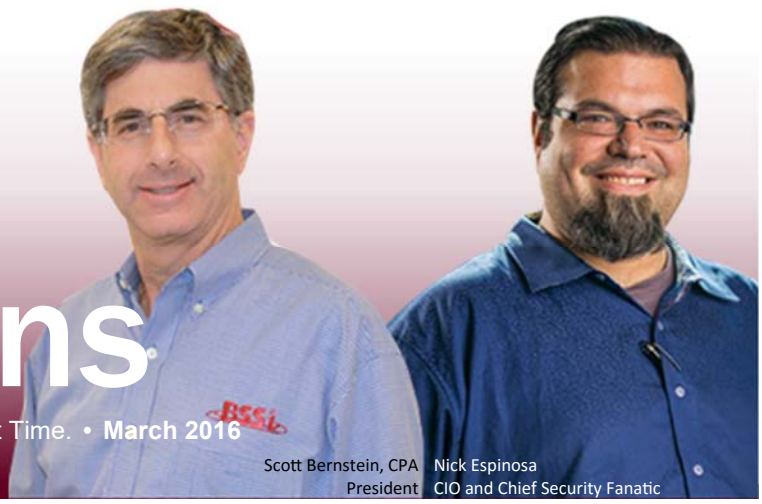
BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time. • **March 2016**



Scott Bernstein, CPA
President

Nick Espinosa
CIO and Chief Security Fanatic

The Lighter Side….

Adult Truths:

1. Sometimes I'll look down at my watch 3 consecutive times and still not know what time it is.
2. Nothing sucks more than that moment during an argument when you realize you're wrong.
3. I totally take back all those times I didn't want to nap when I was younger.
4. Bad decisions make good stories.
5. You never know when it will strike, but there comes a moment when you know that you just aren't going to do anything productive for the rest of the day.
6. Can we all just agree to ignore whatever comes after Blu-Ray? I don't want to have to restart my collection... again.
7. I'm always slightly terrified when I exit out of Word and it asks me if I want to save any changes to my ten-page technical report that I swear I did not make any changes to.
8. I keep some people's phone numbers in my phone just so I know not to answer when they call.
9. I wish Google Maps had an "Avoid Ghetto" routing option.

Tech Imitates Life: How One Human Vulnerability Compromises Network Security

Nick Espinosa has recently became an author for SmartFile.
Check out his author page and other articles he's written at:
www.smartfile.com/blog/author/nespinosa/

My local supermarket is usually where I buy alcohol. Almost without fail, my purchases are rung up by someone not old enough to legally drink. As a result of this, every time I buy alcohol, the teenage cashier has to call for Customer Service to come and check my ID (which is no longer flattering at 36, trust me). They swipe the bottle through the scanner and then hand it back to the teen who then puts it in a bag for me.

Most people don't mind the delay. We've all accepted that this is a safeguard to ensure that teens cannot sell alcohol to other teens and also to make sure ID is checked. Putting on my IT Security and Analytics hats for a moment, I start to find flaws in this process.

The cashier can quickly inspect and validate all of my items, efficiently processing them so I can pay and take them outside of the secured perimeter of the store. When alcohol appears, this "firewall" understands that this is traffic it's not allowed to inspect, so it forwards the request to the Threat Management system, aka Customer Service, who will then validate the request for purchase.

This process is essentially the nuts and bolts of a perimeter-based security system in a network. This is also a deeply flawed process that leaves large portions of the network exposed to attack and can also allow viral infections to spread.

The Major Flaw of Every Security System

Tech security is built by humans, and it's in our nature fall back into old patterns for verification. We've been doing this for thousands of years, from the old counting system of putting the product count in a sealed jar and sending it with the shipment for the receiving end to verify, to having to go through a body scanner at the airport. Pick virtually any major security or filtering method we, as humans, have employed and you will find one common issue between all of them: trust.

By nature, we are inherently trusting people. Depending on the security system, we rely on at least one element in this process of verification that is based purely on trust. For instance, Customer Service at the supermarket trusts the teen to alert them to an alcohol purchase, bag it and give it to me once I've paid. Some systems will not allow the teen's login to accept alcohol, some will not, however, both methods employed still have the teenager handling alcohol in the process.

Buy a ticket at a movie theater and beyond checking the ticket when you walk in, the theater trusts you not to be armed. At the airport, the TSA trusts that the general public is not capable of disassembling and hiding weapons in such a way that a worker paid slightly more than a fast food employee can't detect it.

These varying degrees of trust are based on necessity, cost and also logic. A movie theater doesn't need an armed brigade to body scan every patron because the chance of a serious ...

Continued on the next page

incident is very low, despite the horrible situation in Colorado a few years ago. However, an airplane can be hijacked and used as a weapon. Hence, the greater the risk to humanity, the less trust the security team and filters should have.

In both cases, cost is weighed into this as it relates to the severity of possible threat. Movie theaters do not spend a good deal of money on security beyond a few guards or employees checking to ensure the person has paid, and this is usually fine. Movie theaters tend to be safe and are considered low priority targets, so security can be lax and it's usually not an issue.

Securing an airport, however, is a different animal. A good deal of time and money is invested in ensuring that points of entry into the airport are secured, guarded and blocked. Equipment is purchased to scan and check all passengers and personnel coming into the airport. The real threat of terrorism against our air transportation infrastructure warrants the sometimes outrageous cost to ensure security.

Unified Threat Managed Firewalls > Perimeter-Based Firewalls

So, why are corporations overwhelmingly leaving their computer networks open to attack by running a network security philosophy that is flawed by trust and antiquated? Perimeter-based firewalls only check traffic in, and hopefully out, at the perimeter but do nothing to check internal communication between computers, devices and servers. It is trusting and authenticating computers when it's very possible it shouldn't be.

Unified Threat Managed (UTM) firewalls are better in that they're validating inbound and outbound traffic against known threats. They look for patterns and data that could signify infection or malicious intent, but like a standard non-UTM firewall they do nothing to check and protect computers within the network while they're communicating.

Locally installed virus scanners are notorious, despite their own claims, for catching only a fraction of infections; they miss Crypto malware and usually lag 24 hours or more behind in definitions because of how the virus companies release updates. Most UTM firewalls are also in a very similar boat though that is changing thanks to a few leaders in the field and the increased competition to put forth a truly secure UTM firewall.

The truly best security posture an IT security professional can take is to see the flaws of these conventional configurations in the networks they manage. They need to realize that the only true stance is to divorce themselves and these networks from what has held security back for ages: trust. Networks need to be the tinfoil-hat-wearing, "everyone-is-out-to-get-us" paranoids. Everything is suspicious and should be treated as such.

The Zero Trust Model

A while back, Forrester Research came out with such a model. One that has been proven effective time and again and should be applied to all networks and infrastructure that need serious defense. This model is simply called "Zero Trust" and it's as simple on paper as it sounds.

A network with Zero Trust assumes that all computers, servers and devices within the defense perimeter are threats, as well as threats to everything else, before they prove themselves. In essence, every time a computer wants to talk to another entity on the network within the perimeter, that traffic is analyzed for threats via an internal firewall that updates itself throughout the day with the latest intelligence and virus definitions.

This updating, known as Zero Day, requires the firewalls be from a company that is constantly sandboxing and analyzing threats in the cloud. They then write inoculations for said threat and immediately push them to the firewalls globally. This defensive stance enhances security and filtering drastically in that the time it takes from discovery of a threat to inoculation of the network can be as fast as half an hour if it's coming from a top tier firewall provider.

Typically, in a Zero Trust network with Zero Day updating, a crypto infection cannot spread beyond the infected computer, meaning that server shares and other assets are safe from attack. Think again of being in a supermarket — every time you add something to your cart, there is a security guard there checking what you added and making sure you didn't pocket it instead.

Application Whitelisting

Yet…this isn't paranoid enough. Threats can still slip through even though we've vastly mitigated this possibility.
Enter Application Whitelisting. On top of the internal firewalls scanning all traffic for threats, the best firewalls will also do Application Whitelisting so only allowed traffic can pass through the firewalls.

For example, if a network only allows 3 applications to be used on its network, then why allow all other traffic as it could be potentially malicious? It cuts down on network traffic, and those whitelisted applications are still scanned for threats because while they're allowed through the firewall, it doesn't necessarily mean they're clean.

This stance is the best possible method to ensure no threats can go in and out. This would even apply to mobile devices like phones and laptops that should be connected and running their internet traffic through a Zero Trust, Application Whitelisting firewall via a VPN connection 24/7.

Clients with this level of security don't get infected. They simply don't. This is like going to the grocery store and before you enter, Security approves your shopping list, follows you around the store checking you constantly so you can't deviate or try to sneak something into your cart and then walks you to your car after helping you check out. The odds of infection are so incredibly low that we never have to worry about it. Investing in a network that has this level of security is obviously more expensive than simply buying a firewall, but it pays off in the long run since no time will be lost to infection cleaning or lengthy restorations of data.

When you're planning or reviewing your IT security remember that you're only as strong as your weakest link. Don't be the supermarket.

This article was published 3/14/2016 through SmartFile.com

Relying On A Good Luck Charm?

Carrying a four-leaf clover might work for leprechauns. But when it comes to Internet abuse by employees, you're gonna need more than sheer luck…

Did you know that…

- 70% of all web traffic to Internet pornography sites occurs during the work hours of 9 a.m. – 5 p.m.
- Non-work-related Internet surfing results in up to a 40% loss in productivity each year at American businesses.
- According to a survey by International Data Corp (IDC), 30% to 40% of Internet access is spent on non-work-related browsing, and a staggering 60% of all online purchases are made during working hours.

The list goes on, and the costs to your company can be staggering.

What types of web sites present the greatest risk? Categories include abortion, alcohol, dating, death/gore, drugs, gambling, lingerie/swimsuits, mature, nudity, pornography, profanity, proxy, suicide, tobacco and weapons.

Risks these types of web sites expose your business to include malware, viruses, fraud, violence, lawsuits, loss of confidential and/or proprietary data and more. Even social sites, while perhaps not quite as risky, can have a major impact on productivity.

Barriers that once stood at the edges of your office network have been annihilated by digital media.

Web content filtering is now crucial to network security – not to mention employee productivity – in this emerging environment. It can be deployed in a number of ways, but basically they boil down to two: inline and endpoint filtering.

Inline Web Filtering

One way to filter web content is to control it at the entry point or gateway to your network. This technique intercepts all web traffic and applies filters that allow or block web access requests. Because the entire network is filtered, no access to the user's device is required.

With inline web filtering, there's no need to expend resources managing content at each endpoint – your employees and their computers, whether desktop or mobile. Inline filtering not only saves bandwidth, it goes a long way toward mitigating cyberthreats. For securing activities that take place within your network, it's a critical and potent strategy.

Yet, with the shift away from traditional office-bound work routines to a work-from-anywhere culture, the effectiveness of inline filtering has diminished. When employees access the web outside your network's gateways – via home networks, hotels, coffee shops, etc. – their devices become vulnerable to attack.

And any employee can carry an infected machine into and out of your company's building and network on any given day, exposing your entire intranet to infections. And that's why so many companies are moving to endpoint-based web filtering to complement their inline filtering.

Endpoint-Based Web Filtering

Endpoint-based filtering protects employee devices from infections, no matter where they connect to the web. Software at the endpoint – your employee's device – carries a predefined filtering policy from the central server that can be intranet-based or cloud-based.

The endpoint filter is then updated periodically from your company network. This method assures that web filtering is always active, no matter which gateway the machine connects through. The downside is that it must be rolled out and maintained at all endpoints.

That being said, one advantage of endpoint-based filtering is that it addresses stringent employee privacy regulations that are quickly becoming the norm in Europe and elsewhere around the world. Because it keeps browsing-pattern information within the user's device, endpoint-based filtering provides a fairly non-intrusive way to handle employee privacy concerns.

And finally, while endpoint-based filtering really is the only way to protect a network without boundaries, as most companies now have, ideally it works hand in glove with inline filtering.

Forget the Charms – You Can Bet On This

We highly recommend rolling out not only inline and endpoint filtering, but also an effective training program for your staff to encourage best practices and assure compliance with your company's web security policies and procedures.

March 2016#

35 Aztec Court
South Barrington,
IL 60010

(847) 551-4626

www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Shiny New Gadget of the Month

New App Tames Expense Tracking

Business Travel and Entertainment is one of those expenses that can bleed cash from company coffers – IF you or your CFO don't keep an eagle eye on it.

And no wonder: it often entails hand-entered data, widely disparate vendors, no real time reporting and, until now, an out-of-office transaction with no mobile reporting back to a central corporate database.

Enter Concur. This automated, mobile expense management system lets business travelers focus on their jobs while giving finance leaders complete and real-time visibility into spend.

It automatically captures and categorizes company credit-card transactions, making it simple for traveling employees to review, reconcile and submit statements for approval.

At the same time the immediate insight it provides helps you and your finance team stop bad spending decisions before they happen, manage budgets more effectively and drive better business performance. Learn more at Concur.com.

"People find coloring soothing, so I've printed some copies of this and passed out crayons for everyone."

Meet Rose Avila, BSSi2 Service Manager!

Effective March 17, BSSi2 has a new service manager: Rose Avila. Rose has worked many years as a service manager for IT companies and we are thrilled to have such an experienced person looking out for our clients and technicians. You will continue to use the same phone number and email for support. Please welcome Rose to our team!

Mike Carrington and Jennifer Hembd-Johnson are still with BSSi2, but in different roles.

BSSi2 Support | (312) 752-4675 | support@bssi2.com