Slide: The Threat Landscape

Security threats come in many shapes and sizes these days. I'm sure you've heard of the many high profile data breaches like Target and Sony. The theft was really bad but the PR nightmare these companies have to endure makes it so much worse. The reason these companies were susceptible to these attacks can be summed up in a single reason: too many types of threats and too little time to mitigate them.

Let's put that into context a little bit. Threats are changing fast. Attackers are coming up with more ingenious ways to exploit vulnerabilities faster than ever. According to the Internet Security Threat Report that's released every year by Symantec, the discussion is turning from "threat X and exploits a vulnerability" to "vulnerability Y is used by these threats and in these attacks".

There are countless ways for the bad guys to compromise a network and steal whatever they want. Malware is a huge one. I'm talking about self-spreading worms, viruses and the like. Malware can be delivered in lots of different ways and the bad guys are continually testing out different ways to do it. At one point, you could simply port scan a company's firewall, find a vulnerability and send it through. That attack vector has been taken care of now for the most part so they go the route of social engineering tactics through sending emails with enticing links for users to click on, they leave USB keys laying around for curious employees to stick into their computers and a whole lot of other ways. They're essentially preying on simple human curiosity and it still works!

This malware is also becoming smarter once it's delivered. It's becoming more adaptable to the environment that it interacts with. For example, according to that Internet Security Threat Report, up to 28% of malware now is even virtual machine aware. There's even one called W32.Crisis that even detects if it's running on a virtual machine and then immediately tries to infect other VMs. There goes your attempts and spinning up a VM to test preventative measures.

Ransomware is another big one now. Have you ever encountered CryptoLocker? I hope not. CryptoLocker and it's variants is software that gets delivered onto a computer, automatically starts scanning that computer's hard drive and even all of the network drives and then immediately encrypts everything with a key only the attacker has. Technically, you could consider it a worm due to it's self-spreading behavior but it's a worm that owns your data as fast as it can!

I personally have known companies and individuals that have actually paid these guys to get their data back since they didn’t have any backups. Once an attacker is in, consider your data there's to do whatever they want to do with it! Always have offline backups. Always! It may be a pain to restore that data but at least you don't have to pay a ransom to get it back! Ransomware is said to be a multi million dollar business now.

The truth is, attackers are simply moving faster than most defenses. It's always been a cat and mouse game. The good guys will always be at a disadvantage since they're always playing catchup trying to patch the next 0 day vulnerability that comes down the pike.

Slide: Threat Origination

Once upon a time threats all came from the Internet. I remember the days of detecting port scans on my external firewall all the time noticing presumably bots just poking around to see what they could find. This still happens today but it's such old practice that just about every firewall has incorporated some preventative measures against this. Attackers have had to adapt.

They're now using phishing attacks through email that look like legitimate email from banks or even from internal IT security asking them to reset their password. Sometimes, without an organization's security training, people will fall prey to these attacks and willingly give up their password and lots of other internal information. Who doesn't want to help IT security, right?

Social networks are another attack vector nowadays. I bet 90% of the people on this webinar have some form of social media account. Attackers are now placing malicious code in Facebook ads to get your click on them. To an attacker, it doesn’t matter what venue the is. It's all about that old marketing adage that says "go where the eyeballs" are. Eventually, if a service becomes popular enough you'll see find some kind of malware or malicious technique designed around that service. It's important to have something in between you and a site like Facebook that's constantly scanning for known malware to catch that stuff before it ever gets to your computer.

Next is BYOD or bring your own device. What was once thought to be crazy talk by internal IT teams is now coming to a reality. People want to use the devices they are comfortable with. This not only saves the company money by cutting down on equipment costs but also makes the employee more productive. They already know how to use their device. Why not provide them with a secure platform to grant them access to company resources?

Business-wise, that makes a lot of sense but since these devices consistently go off the network and are used for personal things IT can never be sure what's actually running on them. This is why some companies segment them off into their own VLAN and provide a separate wireless network with restricted access to internal company data. In any case, BYOD although a big business benefit is another threat that your organization should take into consideration.

And finally, wireless threats. A lot of clients are part of a wireless network. I just spoke about the BYOD movement where things like laptops, iPads, iPhones, etc may get onto your internal wireless network. I'm not talking about threats from the client but rather threats from device intercepting that wireless communication. Here's a picture of a device called a WiFi Pineapple. This little device can be placed in the proximity of your clients and spoof your own wireless network. It can be configured to perform man in the middle attacks which essentially routes all of the information coming from the wireless client through it, records it and then just sends it off to it's intended destination all undetected. The wireless client thinks that it's talking to it's intended destination but it's really not.

Slide: How to Discover Threats

Now that you've got a basic understanding of the threat landscape and a few of the kinds of attacks that are out in the wild today, how do you do discover these threats anyway? Well, you need a system that gets between your users and the threats. But, as you've learned, there's a lot of different threats using a lot of different techniques and protocols. Threats come from simple web browsing, email communication, simply connecting to a wireless network and more. You need something that's able to sit between all that stuff and protect your users. This is typically a single or set of appliances like Dell Sonicwall's solution, for example.

Once you've got something protecting your users you need to be sure that the device can be more than something that simply assumes malware fits in specific molds. As you've now seen that malware is ever changing. You need something that does deep packet inspection. This means not just looking at packet headers but looking at the payload itself and looking for anomalies. Attackers are constantly trying to tweak their attacks just a little bit to fly under the radar. You need something that doesn't just take a quick scan of a packet, doesn't see anything obvious and lets it go through. You need something that looks at every level of the packet.

Also, nowadays, attackers are trying to get around security defenses by encrypting their traffic or by piggy backing onto existing encrypted traffic. You need something that can decrypt that traffic and take a deep look for any malware. Using a security appliance like a Sonicwall that's possible. This gives a positive spin to a man in the middle attack. Traditionally, man in the middle attacks are what attackers use to capture communication from point A to point B. However, the good guys can use this as well. By pointing all Internet traffic to run through the appliance and assigning a certificate to the appliance, it then has the ability to decrypt all SSL traffic which has traditionally been hidden to IT security.

Slide: Layers are Necessary

As I mentioned earlier, attackers are getting smarter every day constantly trying new ways to steal personal and company information. There's no way to put up a strong resistance by simply depending on a single layer. Good security is about layers. If you're familiar with the OSI model, it has 7 layers coming from the electrical signal of the cable on layer 1, to a frame on layer 2 to a packet on layer 3. It's a way nodes have been communicating with each other for many years. Good security measures account for every layer of the OSI model.

This means not only having an Internet-facing firewall that's preventing communication coming in from the outside by also monitoring internal to external communication as well. It's about ensuring that not only is your firewall blocking access at the port level but also blocking access at the protocol level as well as at layer 7 of the OSI model which is the application layer. This is the layer where most malware is transferred. Malware packets match specific patterns. It's important for your security solution to not only account for these lower layers but to also scan for the patterns that malware exhibits at the higher levels. This is done through deep level packet inspection.

SPAM filtering: this is an example of layer 7. A popular attack vector is email through phishing attempts. For example, email can use ports like 25 for SMTP, 110 for POP or 143 for IMAP. SSL or TLS encrypted email with TCP ports like 465, 993 and 995. Your company wants to get and send email, right? You must allow that port open so your layer 3 protection isn't going to apply here. You need something that can scan at that higher level and check the mail headers and contents of the email to catch those phishing attempts before they reach your users' inboxes.

Slide: Controlling Internet Usage

Finally, although not directly related to security is monitoring and controlling Internet usage.

Controlling your employee's internet usage has two main advantages; increased security and productivity. You should have a solution that's able to blacklist known malware ridden sites. By blocking sites at this level is much easier than forcing deep packet inspection if the site is allowed through. It's much easier to simply say block all traffic from [www.attackersite.com](http://www.attackersite.com) than allowing the site through and inspecting every single packet that comes through.

Second is the productivity aspect. A common practice of companies is to block access to sites like Facebook, Twitter, youtube and so on. If you know that your employees will never need access to these sites it's best to practice a concept similar to least privilege. Least privilege, in the security sense, means that you should grant the minimum amount of privilege to users and no more. If you know, for a fact, that your users will never need access to these sites, you can go ahead and block them. This not only prevents any kind of malware coming from these sites but also potentially increases employee productivity because they won't be tempted to waste time on these sites.

One last thing to mention is QoS or quality of service on your Internet link. I'm sure casual web browsing is going to take a back seat to a VPN connection to a remote site right? I'm also sure you'd rather not have someone's download of the newest iOS version for their phone to be hogging up all of the bandwidth and making your VOIP calls drop. Be being able to control things at a protocol level allows you the control to set priority on business-critical communication over less important communication.