

Insider Threat Talk: Q&A

January 21, 2010

- Insider threats have been around, but why are they particularly worrying now?

A poor global economy means people are uncertain about their future employment in many cases, and some will have immediate financial concerns. So the individual threat is higher, because external forces are greater right now. At the same time, new technologies like social media and collaboration tools allow employees to execute Internet code on their desktops, often bypassing traditional desktop security.

- Over the last couple of years, how have you seen these threats change or evolve?

As far as dealing with malicious insiders, the threat of intentional abuse has risen in volume, but the threat isn't remarkably different. I think the threat is greater, however, when it comes to how the insider uses new technology. Rather than attacking the OS directly, we are seeing a lot of attacks against third-party tools. The rise in attacks against the PDF format has risen sharply, for example. This is because people are accustomed to patching their operating system more frequently, and keeping their antivirus up-to-date, but they may not keep these other tools patched. I also mentioned social media and collaboration tools. Various runtime environments, used by developers, can introduce new threats directly to the desktop.

- Are organizations accounting for these changes?

I think organizations recognize the importance of taking inventory of applications on their client machines, and they are trying to keep third-party applications patched. Products like Adobe Acrobat, Silverlight, Java Runtime Environments, QuickTime, etc. Organizations should also be making their users aware of new threats that may come through social media, and phishing attempts through e-mail. Many people use URL shorteners, but not many think about what the real URL might be behind that shortened address, and what malware might be waiting for them when they click on it. I think progress is being made, as long as organizations can manage the threats introduced by new technologies, but that will get more difficult as the perimeter we rely on to protect us erodes, and as technology comes at us faster in the future.

- What are, say, the top five steps information security leaders can take to ensure critical data isn't compromised by insiders?
 1. Develop strong access controls and periodic review of insider access.
 2. Encrypt sensitive data at rest and in motion.
 3. Evaluate the security risks posed by new technologies and develop a mitigation strategy before introducing them to your organization.
 4. Leveraged layered security, involving people, processes and tools to keep risks in check.
 5. Keep your employees informed and educated. Engaged and empowered employees are less likely to pose an insider threat.

- Let's talk a little more about mobile security issues with the insider. iPhones, for example, and other tools consumers are bringing into their workplaces don't lend themselves to centralized management. So how should you best address this problem? What tips do you have for folks?

Mobile devices are a difficult problem. Management tools, particularly security management tools haven't matured as rapidly as we'd like. You can't stick good endpoint protection on them yet, because the mobile devices aren't that capable of supporting background apps that can be pretty CPU intensive. Fortunately, the threat isn't as great as it is with laptops yet. In the next few years, I am sure the capabilities of mobile devices will surpass what we have on our desktops today. A big factor is battery life, so as long as that's an issue, smart phones will be less capable than laptops or tablets.

You have three main platforms: Windows Mobile, Blackberry and iPhone. Internationally, Symbian and other platforms are popular. Nokias are quite popular in Europe. So, if you want to really trust mobile devices, you need security management tools that will enforce the same rules on all these platforms. Since we can't quite do that, we look for something that all of them come in contact with, and that's Exchange. Employees want to synch email and calendar and contacts, and if they want to do that, they're going to get a security policy pushed at them that includes at least screen locking, encryption and remote wipe. Since we can't do much more than that, we should also have a provisioning process that ensures our users are using approved devices that are company-owned. We also need to communicate with our end-users better. Leveraging these tools, we feel we can secure provisioned mobile devices adequately for Exchange, but we will need to keep these phones on the Internet. If we want to start letting them connect to our internal resources, we can't trust them like we trust our laptops, so we need to vet them when they come in, something like we are already doing with remote supplier access.

- When it comes to insider attacks or threats can you provide some anecdotes that you think especially illustrate some of the challenges in this area that you and your peers face? How should one address these?

Let me give an example, dealing with mobile devices. Managers are always looking for ways to cut costs, so one idea might be to eliminate the data plan and then just synch smart phones with Exchange when they are tethered to our desktops. That sounds good, but that ends up bypassing our security controls, because tethered devices don't have the Exchange security policy pushed to them, so we can't be certain they are encrypted, properly locked and secured.

- We've been hearing more and more about cyberespionage threats. For those criminals engaged in this type of activity, how are they leveraging insiders? What can one do to combat this?

External forces, like the economy, can be used to turn insiders. That is true whether you are talking about physical or cyber threats. The larger threat, as I see it, which is harder to manage is how we allow our insiders to leverage new technologies and not "accidentally" introduce malware into our environment that surreptitiously gathers information and sends it to agents on the Internet. Employees may even disclose information as they use Twitter or Facebook, to talk with co-workers. I'd suggest to address this, there should be good endpoint security. It's good to place restrictions on the use of technologies like Instant Messaging. We should be more vigilant on how we filter email and proxy websites. And, organizations should develop a social media usage policy, and communicate that to insiders. If a new threat is spreading in the wild, it may become necessary to block access to Yahoo and Gmail and social media sites, until there is more information. New threats develop very quickly in this space, and the recent attack on Google is just one example. We have to expect that there will be a period where there are few or no ways to mitigate these risks with a technical solution, and that's where education comes in. Most users want to do the right thing.

- I saw a press release the other day about an increasing number of incidents occurring in the UK where employees have been leaving USB sticks in clothing that they've taken to the dry cleaners – some of it PII. Of course, it was lost and there were a few instances of fines. What can companies do to deal with USBs?

We should be sensitive to how we deal with insider threats in different cultures. I mentioned that gaps expose themselves as you expand globally or into new markets. Not all cultures treat proprietary data with the same care, so I can think of cases where we simply don't allow the use of USB sticks. This isn't a very fine-grained way of dealing with the problem. I think ideally we'd want to employ some kind of DLP to monitor and record how data is being used, so we can protect it appropriately and still allow the business to leverage these new technologies productively, as opposed to such broad brush techniques. If you don't have the budget for full-blown DLP, even just developing and communicating an encryption policy to your users, explaining when to use it and how to protect data better would be an excellent start.

- What other tools that make employees' lives easier end up a huge threat to the company?

I'm sure many of you have heard of the data breach at Twitter this last year. It points out the risks that come with jumping on the cloud computing bandwagon, without considering the security consequences. This is a fairly simple case of someone using the same password in multiple places, but they were storing sensitive files in Google Docs, and these files were exposed because a flaw in another social media site exposed a password, and this got the attacker onto other sites, like Google. Just think how many of our insiders use the same password in many places. I have found about 40 social media websites, and I'll bet you that the average user would expose all of them, if just one had a vulnerability and their password was hacked. The point is, if a company wants to adopt new technologies, like cloud computing, there may be a way to do that while managing the security risks, better than if they just take a new technology and "throw it over the fence" and see what happens.

- Information security pros want to be seen as enablers more than ever, so how do you enable staff to use these various applications and tools but still ensure data is safe?

I doubt there are any technologies that are risk-free. On the other hand, I doubt there are any new technologies that can't have their security risks evaluated and mitigated to some degree by leveraging people, processes and tools. Since there is often a lag, getting tools that will mitigate these risks, there are going to be cases where the business may choose to wait, rather than adopting them right off. There is a lot of pressure for business leaders to identify new technologies that will give their organization a competitive advantage, so it is increasingly important that security be seen as a partner that is involved in evaluating these technologies early on. It is the job of the security professional to assess and make recommendations, based on their risk analysis. If the business hears this clearly, then it is their decision as to how much risk they decide to accept. Business leaders are used to risk management, and usually act in a prudent way, so it is the responsibility of security to keep them informed and communicate in language that they will understand.

- Economy's been tough... do you have any advice for your peers about ensuring they get the budget and resources necessary to meet critical security goals this year?

I'd say that it's more important than ever to get your ducks in a row before you go asking for money. Perform a risk analysis. Think through the details. Give business leaders options. Avoid overly technical jargon, and put things in terms of cost avoidance and learn to speak in their

language. They need to see how security is distinct from other IT programs, and they need to understand the consequences of ignoring security. The numbers bear out that this message is getting through. Good managers don't arbitrarily cut their security budgets, and we see evidence that security budgets tend to fare better, in a down economy, than other IT departments.

- What are your key detective controls for insiders with administrative privileges?

I think you start with separation of duties, and give people the access they need. This is difficult in practice. I feel large organizations really need to have a program to address identity management. Because of Sarbanes-Oxley, I think many organizations are more sensitive to this problem and have started down this road.

It is possible to develop artifacts, based on active directory groups, logs and security events. You might put centralized security logging and event management in this category, as well as DLP or even NAC. Log management is not a simple task, though, when you have lots of data to sort through. You might take the approach that you put this kind of data in front of responsible managers, and have them sign-off on access rights and the efficacy of any controls they are responsible for on a semi-annual basis. This is very reactive, but it may be all we can do, today. I don't think IDS works very well, on the inside. If you give people the access they need to do their job, then how do you programmatically tell the difference between their normal duties and abuse?

I'd like to see the tools we have today, evolve into something that is "smart" and can look at what users are doing in real-time and compare it to a baseline of their normal behavior, and when they act outside of some norm, they are asked for stronger authentication, and so on. I feel confident that in another ten years, we will look back at the tools we use today, and feel they are too slow, too course grained and not proactive enough. I think that's a safe bet.