Defending the Network: Cyber Threats of Today

Ian Burke
Regis University
MSIA 676

July 30, 2011

Abstract

Every organization has a different focus. This is what makes them unique. Whether it is the product that they produce or the method they employ. This also changes the threat vectors facing the company. Awareness of those threat vectors is essential to defending against them. It has been said that there are five major areas of attack that industry needs to be concerned about over 2011: supply chain, mobile devices, targeted attacks, political attacks, and cyber war. Some typical concerns that also need be protected against include insider threats and malware. Protecting against these threat vectors is both an important measure as well as a relatively simple thing to accomplish.

Discussion

Threats today are no longer attacking random targets. Attacks today are targeted and economic motivated. Because of this as organization looks at the threat vectors facing their network they must consider the assets that they are defending. This provides insight into how to defend the different assets. Looking at supply chain threats we can see that there is an opportunity for products, such a software, to be modified between the production controls and the customer. The delivery chain provides multiple opportunities for modification to a product. Vendors have quality controls in place to ensure that a product meets their appropriate safeguards when it leaves the production line, but there are many other players that interact with a product between the manufacturer and the customer. Lets look at the typical server. How often is a server driven by IBM employees from the IBM assembly line to an IBM customer? Your typical supply chain will involve shipping companies, third party vendors, and often even contractors that may install and configure the servers for the client. In the event that the server is being customized for a specific application, say a radiology system, the vendor may even be re-branding the IBM server under a different label. In any of these situations there are many other parties that have the opportunity to bypass and violate the quality assurance provided by IBM. So what is the threat, you may ask? If IBM does not have control of the system the potential for a root kit to be loaded in the bios or for a compromised OS to be loaded on the system is ever present. Today's attacks are targeted and with purpose. We do not have to look that far back to find example of such an attack such as the digital picture frames that were distributed a few years ago loaded with malware.

So how do we defend against such an attack? Common practices such as flashing a bois with a current version and re-imaging drives of new systems will help to prevent many of these supply chain attacks. Other threats, through peripherals such as thumb drives and picture frames, where these threats might be more prevalent, can also be curtailed with best practices such as limiting the use of these devices on the network. If users need the use of a thumb drive then they should be vetted and provided by the IT department of the corporation and not brought in by each individual.

As we look at devices such a thumb drives we realize that data is becoming more mobile than it ever use to be. With mobile device: cell phones, smart phones, tablets, laptops, and other portable data devices, infiltrating our networks, our ability to control the flow of our data and conversely secure the data has become that much more difficult. Policy, backed by appropriate education, is certainly the most important tool we have in our arsenal. Beyond that, tools such as data loss prevention technologies and data monitoring technologies, including encryption, monitoring and device control technologies.

One of the key issues around mobile devices is how people use them. As users become more mobile they interact more with critical corporate data through their mobile devices. Whether it is email or file access or web surfing, each day more data is being accessed through mobile devices. Educating users to know what data can be stored on these devices is critical. Stopping confidential data from transferring to the device long before technical safeguards are employed could be the difference between secure and breached data. Users also need to know when they do have confidential information in their mobile devices. Many of these devices have the ability to be remotely wiped. Many encryption tools also add a similar functionality. Maintaining control over a device and awareness of what information is on the device is important.

As mobile devices become more prevalent we are also seeing new attack vectors show up across this space. Many of these devices are ill equipped to prevent an attack. With the lack of anti-virus software and poor or absent encryption options available on many of these devices, we are seeing the emergence of new threats to these devices directly. It is becoming more important to architect the network so that these devices are removed from the critical data. Most of these tools do support VPN solutions and those that don't can be relegated to web based resources.

As was mentioned, attacks today are more targeted. The attackers are more skilled and generally have more resources than they did before. If an determined attacker wants to get into a target there generally is little that can be done. Fortunately, while those statements are true, we also are seeing that these targeted attacks are economic driven. If you can raise the cost of entry they generally are not going to make the effort. While most attacks are targeted. They often will have chosen the target due to an opportunity. Removing those opportunities is essential. Keeping systems patched and basic security standards in place will deter most attacks simply because the costs are too high. Often it is not the getting in that is the difficult for these attackers, it is the getting the data out that is more difficult. Just as with any business, attackers have invested into their resources that they leverage in an attack. While they may be able to penetrate your defenses, they spend a great deal of energy ensuring that they leave no traces so that their resource pool is protected. This is where your security systems can be leveraged to make the removal of data more difficult.

This becomes more difficult when the attack is no longer an attack of opportunity but rather a political or business motivated attack. Attacks such as the Lulzsec attacks on Sony, where the group had a political agenda and a chosen target, are difficult to defend against in large part because the motivators may no longer be economic and when they are they often are significantly greater then the cost of being identified. These types of attacks push the envelope of criminal activity to new limits. These cyber attacks which have been more prevalent in the news over the past year are essentially unstoppable. The objective when defending against these attacks is not to stop the attack but rather to limit the damage. Rapid identification of an attack and strong segmentation of critical assets from general data help to limit how much confidential data will be exposed in an attack such as these.

In years past we became familiar with companies such as TJX loosing millions of credit card numbers when breached. Most of these losses were due to poor security practices and or poor network designs. Today whether due to regulatory compliance or better awareness, many companies are better prepared for the typical attack. This is where the work of cyber gangs such as Lulzsec and Anonymous is that much more impressive.

But what if we were to scale these perfect attacks up to not just one business but an industry, or a nation? What if a cyber gang or a nation state were to launch a well crafted cyber attack against the United States financial markets at the same time that the the nation hit it national dept ceiling? Would that be an act of war? These cyber war efforts are the types of events that nations are both afraid of and for which they are preparing. In the wake of Stuxnet, nations around the world are keenly aware that the ability to infiltrate national resources in a critical way is not simply possible but also likely. Defending against these new military fronts has become a new priority for the nations military. It also need to be a priority for our industries.

Ensuring that our individual systems are as robust against attack as possible is essential. While there are national resources that need the support of the military, much of the technology employed by the military is the same as it would be in private industry; the question becomes scale. Monitoring, scanning, and blocking is what provides the awareness that is then leveraged in forensics in the event of a breach. Appropriate deployment of these technologies across industry allow the private sector to support the backbone that the the military and government defend. Perhaps a fair correlation would be to compare private industry's utilization and relation of the larger infrastructure to the user base those industries support. When the users are well educated and employ safe computing practices it is much easier for the individual businesses to protect their respective assets. When each industry employes strong security practices and protects their assets it becomes easier for the nation to defend its national cyber resources.

Conclusion

Perhaps none of us know what the next cyber attack will look like. We here security experts from organizations talk about threat vectors such as advanced persistent threats. And we hear news about new cyber war fronts emerging. What we do know is that the threats facing our networks are changing every day and that employing our best practices some days may not be enough. We also know that that is the best we can do. We need to work with our vendors to ensure that the assets we acquire are secure from the onset. We need to work with our users to ensure that we provide them with the technologies to help protect them and their increasingly mobile and dynamic computing needs. Along with this technology we need to provide those users with the education and tools that equip them to be self sufficient to the point that they can be an asset not a hindrance to the security effort.

Years ago we had the casual hacker simply looking to make a name or themselves or running random scripts. Today attacks are much more targeted. Some are political and most are economic driven. The motivation behind an attack is different and the resources behind an attack is more significant. The net result is that today we may see fewer random viruses and a decrease in some types of attacks but those attacks that are happening are more effective and often more lucrative for the attacker. As we expand the threat vector we also are now seeing the prospect of cyber war as the next great threat facing society today. How we protect our individual assets may play a significant role in how our nations protect the national resources.

References

Andress, Winterfeld. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Syngress, USA.

Baker, et. al. (2011). *2011 Data breach Investigations Report.* Verizon Business. Retrieved from: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report 2011_en_xg.pdf.

Jackson. (2011). *5 cyber threats to Watch Out for This Year.* Government Computer News. Retrieved from: http://gcn.com/Articles/2011/01/17/Security-trends-2011.aspx?Page=1

Jackson. (2011). *How the Most Common Cyber Exploits Could be Prevented.* Government Computer News. Retrieved from: http://gcn.com/articles/2011/02/16/rsa-8-m86-threat-report.aspx.

Pfleeger, Pfleeger. (2011). *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach.* Prentice Hall. USA.