February 2013

Vector

A Net-Square Initiative

A series of articles specially designed for the information security professionals.

Hiren Shah
President, Net-Square
reach him at hiren@net-square.com

Secure • Automate • Innovate

Net-Square Solutions

is a niche Application and Network Security Service provider. Net-Square provides Consulting Services like Vulnerability Assessment, Penetration Testing, Code Review, Reverse Engineering and Security Architecture Consulting

Net-Square also offers Products like Server Defender Vulnerability Protection (SDVP), a web application Firewall for IIS applications and NS Webscan, an automated application vulnerability scanner

Last but not the least, Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

~~*Breaking*~~ *Hacking News:*
Two new security flaws discovered in Java 7 immediately after release of Update 15!

Recently, Oracle released a security patch, Update 15 for Java 7. According to a Feb 27 article in a leading IT news site, tom's IT PRO, as less as six days following the release, an independent security firm identified two new serious vulnerabilities! Oracle has identified these security flaws as "issue 54" and "issue 55". They allow hackers to bypass the Java security sandbox leading to serious issues like viewing and changing user data and execute programs. Our last month's article on Java was so timely!

Hack back?

If there's somethin' strange in your neighborhood, Who ya gonna call? If it's somethin' weird an' it don't look good, Who ya gonna call? These are lines from the famous cult movie of the 1980s called Ghostbusters! You could ask the same question when it comes to the web today, but who you gonna call? Cybercrime cell of the local law enforcement agency? But how will they chase down the guys who are attacking you from a land hundreds and thousands of kilometers away? The attack and the attackers are not their jurisdiction!

Imagine what is the remedy available for an online retailer if its ecommerce website is under attack during the festive season when it does almost 80% of its business. Or a banking institution if it is under attack on a Friday evening when it has the highest volume of online transactions taking place. Unfortunately for all concerned (those who have good intentions at least) the challenge of fending off an attack once it starts is no less than climbing Mount Everest even if they know where it is coming from.

The reason. We haven't responded to the challenges posed by the online world with the same swiftness as is required. To start with we don't even have laws necessary to help people and organizations defend themselves. In fact if anything there are laws, which could land them in trouble, if they attempt to hack back. For example the IT Act in India or Cybercrime law in US, have extensive provisions of what is constituted as cybercrime but none of them have a provision that defines an exception to that definition if the act is performed in self defense or to contain the harm from an ongoing attack by attacking the attacker. In such circumstances if an organization or an individual were to try and stop the attack by attacking the machines which are the source of the attack in an act of self-defense that itself may be categorized as an attack and the individual or the organization may have to face the brunt of these laws. In the hurry to protect individuals and organizations from the attacks that emanated in the online world, the lawmakers were quick to enact these laws as a deterrent. But it seems they completely missed the aspect of self-defense.

I accept that legislating for the online world is not an easy task. In the case of the online world there are no boundaries and very often the attacks are perpetrated by the attackers not from their own machines but from those of other individuals and organizations. Attackers use botnet or zombies i.e. machines belonging to other unsuspecting people or organizations that they have been able to break into and virtually own. Attacking the attacker would mean attacking and shutting down or damaging machines belonging to people who have otherwise nothing to do with the attack.

But aren't there parallels in the physical world. Criminal laws in most countries have express clauses defining what constitutes self defense and upholding the right of an individual to use force in order defend his / her body and property. So let's take an example. If some thieves came on a stolen bike to steal money from someone traveling in a car and in defending himself / herself, if the individual in the car ends up damaging the bike, the owner of the bike cannot lodge a complaint against the person in the car. Isn't this similar to what happens in the online world when the attackers hijack machines and use them to attack others. In the absence of any specific protection in the laws concerning Cybercrime, can provisions from the Criminal laws come to the aid of the beleaguered organizations who when under attack, can attack back to control the damage? Maybe experts from the legal field can throw more light on this.

And it is strange that while laws don't protect individuals and organizations, nations have already started using "hack back" as a strategy to strike back. The stories around chinese and Iranian hackers going after US assets in retaliation to attacks made against their own installations highlight such instances.

So what can organizations do? In light of the confusion in the law and the fact that the business world is more globally connected, organizations need to focus on strengthening their own assets against attacks. Using a "red team" approach is a good idea to evaluate the preparedness to respond to any type of attacks. "Red team" approach is a concept of allowing a team of crack commando style infosec analysts to attack the corporate IT assets to gauge the preparedness of the IT assets to withstand the attacks and also the effectiveness of the incident response process. And who better then the elite commandos of Net-Square to be the "Red team". They are anyways trained to think like attackers!

- Hiren

Follow Hiren's views on Twitter @hiren_sh *or on his blog:* The Thought That Counts

BYOD – BRING YOUR OWN DEVICE

Ask any CISO what his / her topmost concern currently and 7 out of 10 will tell you its BYOD! More than 70% of IT executives believe that companies without BYOD will be at a competitive disadvantage! Before I go into it too much, let me explain what does this term mean. BYOD stands for Bring Your Own Device. It refers to a policy allowing employees to bring their own computing devices such as smartphones, laptops and PDAs to the workplace and connect that to the corporate network in some way.

How hot this topic is can gauged by the fact that only in last one week, we have received calls from five Client CISO's who have asked us for our opinion on the subject. During the same time we conducted Security Review of two topmost BPO organizations in India on behalf of an international Client (lately more and more client's are asking us to do this – helps them avoid a 30,000 kms. journey and we like it as it is a green way of doing security!). And both these Organizations had a BYOD policy. Can you imagine BPOs, who have to implement the highest level of security, feeling the need to implement a policy to allow employees to bring their own device to office.

BYOD surely has its advantages. Employees are happy as it gives them freedom to use their own device, which increases flexibility, convenience and productivity. Companies are happy because it cuts the cost deployment and management of sometimes hundreds of devices. It's not surprising therefore that BYOD has become a natural favorite amongst both, employees and employers. In fact our President Mr. Hiren Shah was a visionary in this regard as he implemented BYOD as way back as in 2006 when he released a policy of allowing select models of mobile phones access to corporate e-mail.

As was the case than, the challenge even today with BYOD remains that of securing the content on the device. As per an article in a Canadian business magazine, www.backbonemag.com, there is a landmark case where IBM allowed 80,000 of its employees to bring their own smartphones and tablets to work. The company soon discovered that it had almost no visibility on the type of applications and services running on the personal devices. There was tremendous lack of awareness of secure usage amongst employees. And this included forwarding internal e-mail to public Web mail services, using smartphones as mobile Wi-Fi hotspots, or storing company files in public, cloud-based storage systems! This forced IBM to develop a clear set of security policies and guidelines, and implement risk free usage such as banning users from accessing free cloud based storage systems, wiping out all BYOD data in event of theft or loss, and also prohibit users from using certain applications.

So what is the answer to this challenge? As we mentioned to the five CISOs who asked us this question, there is no one single answer. BYOD policy will have to be drafted by each Organization based on its needs. But it's important to observe certain principles in drafting that policy.

1. Organization should sandbox Organization's application and data on the device and this should not be accessible to any other application on the device
2. Organization should be able to delete or reset the device completely in the event they perceive that the data and the information on the device is at risk
3. Organization should be able to monitor all that is happening on the device including any back ups or transfers being made by the employee
4. All the data on the device should be stored in an encrypted form and the device should have authorization before the device can be accessed for any functionality at all
5. Connection of the device into the corporate network should be treated as if it is coming from outside the firewall of the Organization

But one key gap we notice in some of the Organizations who implement BYOD is that they have never really tested it. So whether you seek our advise to plan a BYOD rollout or not, one thing we strongly recommend is to get the policy, process and the implementation thoroughly tested. And who can help you do that…….Net-Square!

- *Hardik Kothari, Business Development, Net-Square Solutions*

3rd Party Apps: Secure Enough?

The volatility in the current environment requires business to react very fast to the changing business landscape. And this has to be done not only with speed but also under severe cost pressures. More and more IT teams are adopting 3rd party packaged solutions as their answer to the challenge of providing quick solutions to business. This trend is growing fast in all Organizations. Business are signing strategic IT sourcing deals whereby they hand over the entire IT support to a business process to an external vendor and the vendor takes over the infrastructure and people. Or they are moving to outsourcing model where they buy and customize solutions from a 3rd party vendor for their automation needs. To cash-in on this trend, IT Consulting companies have built products which they customize according to the Client's requirements and implement them onsite. In this process the one piece that gets neglected the most is security. There are no processes/checks in place to ensure the code is taking place securely.

We at Net-Square, while testing applications, which have been provided by 3rd party vendors, were having security flaws, which could have been easily exploited by the attackers to access highly confidential personal and financial data of customers. The story is not different in other verticals. According to a report in online magazine www.SecurityWeek.com, in December 2012, an Egyptian hacker breached Yahoo!'s security systems and acquired full access to Yahoo! Database server. The SQLi attack was carried out on a Yahoo! Web application, which was a 3rd party application.

So how can Organizations protect against this? We at Net-Square had mooted the idea of conducting regular Security Assessment to some of the firms who have many products. But given that there is extensive customization done of these products at the time of implementation, the best practice is to get a Security Consulting firm such as Net-Square to do a periodic code review of the code deployed at the Client end.

The only argument we have heard against this is that very often Clients feel helpless at not getting access to the code. For such Clients, we have good news. We have recently come across cases where Clients are able to get the Vendors to agree to access to code for security code review. Well there is some benefit of this volatile environment.

So next time you sign on the dotted line, make sure you have that clause.