November 2012

V e c t o r

A Net-Square Initiative

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

Saumil Shah
CEO, Net-Square
reach him at saumil@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 is the training programs. Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

~~Breaking~~ Hacking News:

NASA to deploy whole-disk encryption

A recent security breach on October 31st left NASA red faced! A laptop containing sensitive information on a large number of employees and contractors was stolen. NASA says that the laptop was password protected but the information was not encrypted and this would pose danger of the information being available to harmful elements. As a fallout of this breach, NASA says it plans to implement whole-disk encryption on all its employee laptops by Dec 31st.

To read more visit link: http://searchsecurity.techtarget.in/news

5 THOUGHTS TO IMPROVE YOUR INFOSEC MATURITY

As 2012 draws to a close, it is time to start thinking about challenges that the New Year shall bring. As defenses get stronger, so do attacks. 2013 shall be the year of hybrid attacks - targeting man and machine together. The greatest challenge for 2013 shall lie in re-designing your Information Security strategy to measure up to heightened expectations. As you make your plans, let me share with you my top 5 thoughts for improving the maturity of your InfoSec program.

1. Plan on staffing a Red Team

A Red Team is "an independent group that seeks to challenge an organization in order to improve effectiveness". Red Teaming has its origins in the military. In an InfoSec context, Red Teams serve as an "intelligence agency" to identify gaps, vulnerabilities and shortcomings in your organization's IT infrastructure. The sole agenda of the Red Team is to find the holes before attackers do, while continuously coming up with new threat scenarios that impact the organization's IT function.

2. Ensure that all IT purchases require InfoSec approval

There are few tasks more thankless than having to maintain security for an IT system that is defective by design. Talking to our clients revealed that 80% of all vulnerabilities fall under the "we know it already" category. "We have inherited a mess". "We know it is broken, but what do we do?" Do these phrases sound familiar? Well then, make it a policy decision to evaluate and test all major IT requisitions before signing the cheque.

3. Insist upon pre-tested 3rd party developed software

Majority of the vulnerabilities we find lie in 3rd party developed software, or heavily customized implementations of large packaged applications. Shouldn't the software vendor have their software tested for security vulnerabilities before selling it to your organization? It is time to insist for it during the procurement cycle and I would add insist on getting a White box testing certification.

4. Publish a testing calendar for the entire year...and stick to it!

Announce all your vulnerability assessment and penetration testing schedules for the entire year at the very beginning of 2013. Schedule quarterly or half yearly tests for all critical applications, and at least annual tests for all others. Let all your developers and vendors know of the testing schedules. Do not let the testing schedule get sidetracked by release cycles. Software production shall always be delayed. Delaying your testing shall only prolong the agony.

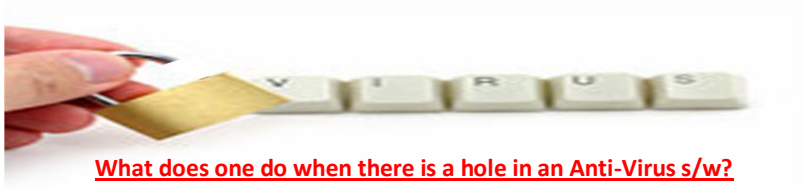
5. Conduct at least one surprise attack on a critical application

Hackers aren't going to wait until after your system migration is complete. Hackers aren't going to spare you during peak transaction hours. Hackers will target your live systems, not your UAT systems. And your IT team will always be stressed - 365 days a year. That is reality. So why conduct fairy-tale penetration testing? As a leader of your InfoSec organization, plan on conducting a surprise attack on the production servers of your critical application during peak business hours. Let me just say that this shall be the shortest path to figuring out the biggest gaps in your organization.

As always, I would like to quote "that which does not kill you makes you stronger."

Until next time, Stay safe!

- Saumil



What does one do when there is a hole in an Anti-Virus s/w?

In most of the cases, whenever there is a new system implemented, or for that matter a new computer installed, the first thing we would go for is Antivirus software. We believe it has to be in place to guard the system against threats, viruses and worms. There is an old saying, or probably a question, which comes to my mind when I think of Anti Viruses. "Who will guard the guardians?" So what does one do if there is a hole in the antivirus software? Is it difficult to believe?

According to a recent article published on 6th November 2012 in an online magazine - theregister.co.uk, an information security engineer from Google, has discovered some embarrassing and critical vulnerabilities in leading enterprise antivirus protection software. The security engineer (while maintaining that his employer has nothing to do with this) has published a paper along with example attack code to highlight the security flaws present in Windows, Linux and Mac OSX builds of this antivirus product. The paper highlights that the antivirus scanner fails to safely examine encrypted PDF's and Visual Basic files, which could arrive in an email or from a website download. These documents can be crafted to trigger flaws within the software and gain control of the system. This makes it very easy for the hackers to exploit and compromise the computer systems guarded by the software.

In its defense, the antivirus company has claimed that the flaws have been rectified a month after they were reported, and that these flaws have not been exploited in the wild. However, the security engineer insists and seems to have enough evidence that the risk is high! One relief here for the antivirus company is that it may not be the only company to face the brunt. In August 2012, NSS Labs, Europe, published a report on the efficiency of protection provided by 13 consumer endpoint protection (Antivirus) products against attacks targeting some critical Microsoft vulnerabilities. The results revealed that when the exploits were served over HTTP, 8 products caught them, while remaining 5 had problems detecting all the variations. Now, when the exploit was served over HTTPS, only four of them continued to be able to protect against the exploit! So how can we protect our systems and strengthen their security?

Antivirus can help you find infected files on machines and probably quarantine them, however proactive protection is something that they lack. As also, protection against exploits of vulnerabilities is not the primary focus of these products. It is best left with the users themselves to protect themselves. One traditional option is to track for patches on new vulnerabilities and install them immediately. The problem here is that by the time the patches come, the attacks are already over and hackers now move on to something new. Sophisticated attackers will not use the commonly available exploits but what they will do is to modify the publicly available exploits and use them against the protection devices. And this cycle goes on.

A better method is to have a holistic approach towards system security. Firstly conduct a regular security testing from the perspective of its usage through Internet and internal functions, which will help to determine security issues and fix them on priority. This will plug the holes from where attacks can happen. Secondly, a security awareness training program for the users of the system will go a long way to protect the system during internet operations, downloads, and other internal installations. And while all this is happening, the antivirus patch management can happen as a continuous backend activity to strengthen security!

- Net-Square Team

Java: Use with Caution!

Java, the widely used programming language by Sun Microsystem (now Oracle) is facing flak once again. Once touted as a "write once, run anywhere" language, malware writers love exploiting Java because it's a cross-platform plug-in. Such an attack vector allows them to target more than one operating system, more than one browser, and thus more than one type of user.

According to an August 2012 report in thenextweb.com, the current flak is due to a new 0-day vulnerability which was founded by FireEye, a US based information security provider. The vulnerability is being used in drive-by download style attacks that eventually result in installation of Poison Ivy remote-access trojan (RAT). If this trojan compromises your computer, it can install Dropper.Ms.PMs with data sent back to separate command and control servers with an IP resolving to Singapore. With the exploit code becoming increasingly available on underground sites, there is a potential danger of increasing the number of infections. Metasploit even has a module available for the flaw!

Affecting all the versions of Java 7, on all the supported platforms, this flaw makes all the browser's vulnerable where Java plug-in has been installed. This means, this will affect all the well known browsers like Internet Explorer, Google Chrome, Mozilla Firefox, Opera and Safari. The worry here is that the fix may not be quick in coming. Oracle runs a strict 3 -month update cycle, and it will take a while before the fix is released. Fearing widespread problems, all the security companies are now recommending disabling or uninstalling Java. Several security firms like Sophos, F-Secure, FireEye have already issued warnings on the Internet. Writes Kaspersky Labs, "The best advice right now is to disable Java altogether if there isn't a pressing need to have it running".

So what should one do if there is a need to access pages that require Java? According to Sophos, "Surf the net using your favorite browser with Java disabled and have an alternate browser available for the occasional site that needs it" Or simply wait for Oracle to come out with the fix!

-Net-Square Team