IaaS Threats In The Cloud – Part 1

Tech Tip
by Philip Cox

© Copyright 2010 SystemExperts Corporation. All rights reserved.
IaaS Threats In The Cloud – Part 1

What are the likely threats in a Public IaaS Cloud offering?

This is part 1 of a 3 part Tech Tip on likely threats in Public Cloud Infrastructure as a Service (IaaS) Cloud. Our last two Tech Tips dealt with threats for SaaS and PaaS Cloud offerings. In the next three tips we will focus on the top Infrastructure as a Service (IaaS) threats you are likely to encounter. In the SaaS model, the consumer was a user, and relied on the provider to secure the application. In PaaS, control (and security) of the application is moved to the consumer, and the provider secures the underlying cloud infrastructure (i.e., firewalls, servers, operating systems, etc). With IaaS, most of the responsibility and control rests with you, the customer. As always, we’ll talk about the threats you can do something about, not those that you rely on your provider to take care of.

What are the most important threats in an IaaS Cloud service?

IaaS by definition includes threats related to PaaS and SaaS. It will also add many other threats because of the nature of the IaaS offering (i.e., you control most of it). From my experience here are the most important threats you’ll have to deal with in a Cloud based Infrastructure as a Service (IaaS) offering:

- Vulnerabilities in underlying operating system and services
- Remote Management: Vulnerabilities in VPN, Remote Desktop, Remote Shell, Web Console UI
- Poor quality credentials
- DNS protocol and implementation flaws

You’ll note that I use the word “important” instead of “likely” in this Tip. That is because at the infrastructure level, the number of threats seem to increase exponentially from the others, and thus while some threats may be likely, they are not as important. This is about remediating the “nasty” ones. Remember that the threats to SaaS and PaaS that we have already covered are still applicable, and must be mitigated.

Threats in underlying operating system and services

The number one threat for the consumer of an IaaS offering are vulnerabilities in the underlying operating system or services that are running on it. At the current time, Linux (and variants) and Windows based OSes are the main options you have in Public IaaS offerings. While other OSes may be available, Linux and Windows are +90% of the market. Both of these OSes and services that run on them have (and will continue to have) vulnerabilities. OS and service vulnerabilities are publicized through many outlets, and in many instances exploits are publicly available. Thus you need to deal with them in a timely manner.

When I talk about OS related vulnerabilities, I am talking about vulnerabilities in core OS functionality such as TCP/IP networking, system calls, system libraries, memory functions, Windows SAM, etc. When referring to services, I am talking about “programs” that use the underlying OS functions to accomplish a task, such as a DNS server, Windows File Sharing, NetBIOS, etc. It is important to differentiate these, as the mitigation strategies may be different. Speaking of mitigation, here are the steps I would recommend (in order) to adequately address these threats/vulnerabilities.

1. **Remove:** First option is to remove the threat.
   a. OS function: For Linux, you can modify the core OS code and rebuild the kernel or system library, then recompile. For Windows, I do not know of a practical way to remove an OS function (as I have defined it).
   b. Service: For Linux, you can remove the executable. For Windows, you may be able to remove the executable, but many services are implemented as part of a single program (i.e., svchost.exe) and thus it is not practical in most instances.

2. **Disable:** The second best option is to disable the function or service.
   a. OS function: Linux, typically a modification of the kernel configuration file, and a rebuild of the kernel. For Windows, this is done through the “Services” snap-in or the “Add/Remove
IaaS Threats In The Cloud – Part 1

Windows components” in the “Add and Remove Program” Control Panel.
b. Service: For Linux, typically done in inetd/rc structure (or equivalent). For Windows, you would use the “Services” snap-in.

3. Block: The third option for those threats you cannot remove or disable is to block access to them. A host based firewall can be used to permit only allowed traffic into the host. You need to understand that while this is effective against all Service related threats, it does not protect against OS functions that the firewall relies on (i.e., a flaw in the underlying network functions will affect the firewall as well). Further, it is important to note that in an IaaS environment, YOU can only use host based firewalls to provide this mitigation. If you rely on a network firewall, then you are putting that control in the hands of your provider (e.g., they are the ones the control any guest to guest traffic on a physical server).

**Caveat Emptor: You need to make sure of dependencies, as removing or disabling functions or services may render your system inoperable. Test it first! Heck, we are talking the Cloud IaaS, this is a PERFECT environment to do this, you can instantiate, modify/break, instantiate again in a matter of minutes!

Next Tip

We have addressed the top threat as I see them in a Public Cloud IaaS offering. Next time, we’ll cover threats in common remote management solutions: VPNs, Remote Desktop, Remote Shell, and Web Console UIs. The last Tip will address threats related to poor quality administrative credentials and DNS protocol and implementation flaws.

Author Information

Philip Cox
CISSP, CISM, PCI QSA, NSA IAM/IEM
Principle Consultant
SystemExperts Corporation
Email: phil.cox@systemexperts.com
Phone: (530) 887-9251