Agenda

Introductions and Internap Overview

Security Drivers and Concerns - Industry Perspectives

Security Risk Evaluation – Service Provider vs. On-Premise

Questions?
Today’s speakers & moderator

Mark Fitzgerald
Manager, Infrastructure & Strategy
Turbine

Marek Vesely
Chief Technology Officer
Casenet LLC

John Freimuth
VP, Mgd Hstg & Cloud
Internap

Randy Rosenbaum
Partner Executive
Alert Logic

Moderator
Our intelligent IT Infrastructure solutions can take your business to a higher level.
We offer unmatched performance and platform flexibility!
Performance to the End user

IP Connectivity
- Enterprise IP
- TCP Acceleration

Content Delivery Network
- Media Delivery, Transparent Caching, Mobile Delivery
- Analytics

Platform Flexibility

Colocation
- Space, Power, Cooling
- Interconnection

Hosting
- Managed Hosting
- Dedicated Hosting

Cloud
- Private Cloud
- Public Cloud
- Cloud Storage

We live and breathe a full range of intelligent IT Infrastructure services
Poll Question

What is your greatest concern about a cloud environment?
What is top of mind today for enterprises regarding security and cloud services?
What business drivers influence your security decisions?
What are your security concerns when using a cloud environment?
Given security requirements, how will you leverage cloud in the future?
Poll Question

Which methods of attack concerns you most in terms of your customers’ data?
Security-as-a-Service solutions for more than 1,500 customers

**Threat Manager**
- Intrusion detection and vulnerability assessment
- PCI Approved Scanning Vendor (ASV)
- Custom dashboards and reports
- 24x7 monitoring and review services

**ActiveWatch**
- Log data collection and aggregation
- Identify suspicious activity and automatically issue threat alerts
- Powerful search and reporting
- Daily analysis and review services

**Log Manager**
- Award-winning web application firewall
- Adaptive learning and easy tuning
- 24x7 monitoring for consistent protection
Industry-First Data-Driven Comparative Analysis of Threats in Hosted and Cloud vs. On-Premise IT Environments

Removal of the Cloud of Insecurity

State of Cloud Security Report

Spring 2012
Alert Logic provides a rich data set
Threat data from more than 1500 customers

Customers of over half the top 30 North American service providers

On-premise enterprise environments from a range of verticals

Consistently-collected data from both service provider and on-premise environments
Customer Data Set

• Analyzed network traffic from over 1600 customers
  – 1300 + Managed Hosting/Cloud Customers
  – 300 + On-Premise Customers
How threats are identified

**INCIDENT IDENTIFICATION APPROACH**

**THREAT IDENTIFICATION**
- Malware
- Network Scans
- Botnets
- Worms
- Trojans
- Unauthorized Access

**AUTOMATED EXPERT SYSTEM ANALYSIS**
1. Attacker Reputation
2. Nature of Exploit
3. Attacker Behavior
4. Target Asset Vulnerability
5. Target Asset Value
6. Global Threat Trends
7. Attacker Confirmation

**SECURITY EVENTS**
- 2.2 Billion

**CERTIFIED ANALYST REVIEW**

**INCIDENTS**
- More Than 62,000
## Security Incident Categories

<table>
<thead>
<tr>
<th>INCIDENT TYPE</th>
<th>DEFINITION</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Attack</td>
<td>Exploit attempts against applications or services that are not running over HTTP protocol</td>
<td>Buffer overflow</td>
</tr>
<tr>
<td>Brute Force</td>
<td>Exploit attempts enumerating a large number of combinations, typically involving numerous credential failures</td>
<td>Password cracking attempts</td>
</tr>
<tr>
<td>Malware/Botnet Activity</td>
<td>Malicious software installed on a host engaging in unscrupulous activity, data destruction, information gathering or creation of backdoor. Included in this category is botnet activity: post-compromise activity displaying characteristics of command and control communication</td>
<td>Conficker, Zeus botnet</td>
</tr>
<tr>
<td>Misconfiguration</td>
<td>Network/Host/Application configuration issues that introduce possible security vulnerabilities, typically a result of inadequate hardening</td>
<td>Weak patch management, unnecessary services running</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>Reconnaissance activity focused on mapping the networks, applications and/or services</td>
<td>Port scans and fingerprinting</td>
</tr>
<tr>
<td>Vulnerability Scan</td>
<td>Automated vulnerability discovery in applications, services or protocol implementations</td>
<td>Unauthorized Nessus scan</td>
</tr>
<tr>
<td>Web Application Attack</td>
<td>Attacks targeting the presentation, logic or database layer of web applications</td>
<td>SQL injection</td>
</tr>
</tbody>
</table>
## Metrics to answer basic questions

<table>
<thead>
<tr>
<th><strong>OCCURRENCE</strong></th>
<th><strong>FREQUENCY</strong></th>
<th><strong>THREAT DIVERSITY</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>What percentage of customers were impacted by each threat type?</td>
<td>How often did impacted customers experience each threat type?</td>
<td>How many unique threat types did customers experience?</td>
</tr>
</tbody>
</table>

What threats are actually experienced in on-premise vs service provider environments, and how often?

What is the complexity of the threat landscape (and resulting security program)?
Consistently lower occurrence rates among service provider customers
Why Do We See Differences?
Size and Diversity Increase Attack Surface

RISK INCREASES WITH SIZE AND DIVERSITY

ON-PREMISE

SERVICE PROVIDER

RISK

SIZE AND DIVERSITY
What does this mean?

Cloud and Service Provider Managed Environments are **Not** Less Secure

Good Management Yields Good Security

Smart Enterprises Should Exploit Differences in Risk Profiles

Web Application Security is a Significant Challenge
Use data to make security investment decisions

This is aggregate data; use your own IDS and log data

- Review log data to detect brute force attempts
- Consider Web App Firewall, network IDS
- Use IDS to detect suspicious recon
- Malware protection critical for on-premises infrastructure
- Pay attention to configuration management, patching

Questions?

www.internap.com
#cloudsecurity