Essential Cloud Security

William Malik
VP Infrastructure Strategies
William Malik Bio

• With Trend since 2017
• In Information Technology for 46 years
  – John Hancock COBOL programmer
  – IBM mainframe OS development
  – Gartner Information Security Service
  – Enterprise Architect/Consultant
Preface: The Architecture of Complexity

Tempus
1,000 parts to a watch

Hora
10 assemblies to a watch
10 sub-assemblies to an assembly
10 parts to a sub-assembly

There Are Always Things You Are Responsible for in the Cloud

**Business Process as a Service**
- Customer reviews delivery against SLAs

**Information as a Service**
- High assurance information
- Customer consumes in their process

**Software as a Service**
- Customer supplies the information

**Platform as a Service**
- Customer builds the application

**Infrastructure as a Service**
- Customer builds the workload
- Customer provides the content

---

You Control It

They Control It
The Perfect Storm for Cloud Security

Exploding set of cloud infrastructure services
DevOps increasing velocity of application delivery
New vectors for breaches
Multiple teams making infrastructure & security decisions
More demanding compliance requirements
Too many security tools
Why Do I Need Additional Security in the Cloud?

**Threats:**
- Network attack
- Vulnerabilities
- Malware
- Insider threats

**Compliance:**
- PCI DSS
- HIPAA
- GDPR
- Internal
Security Challenges in the Cloud

- Visibility
- Agility
- Compliance
- Purchasing
- Sec
  - Dev
  - Ops
What To Do?

• People
  – Awareness and Training

• Process
  – Detection and Remediation

• Tools
  – Keep Software Up to Date
  – Know What You’re Running
Cobit

Then:
This is how to run a data center.

Now:
This is how to manage information technology.
ICT: Cyber Process Hazard Analysis

1. Discover Assets
2. Classify Assets
3. Prioritize Assets
4. Assess Security Posture
5. Build OT Program and Governance Model
6. Design tech and control solution
7. Select implementation partners
8. Implement quick-win solutions
9. Operationalize change
10. Manage steady state
THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. Created with real data by artist Brendan Dawes.
Biography

• Robert O’Sullivan
• 6 Years at Trend Micro
  – IT Program Manager – Responsible for global virtual training platform for all external/internal training labs
  – European IT Manager
  – Cloud Solution Architect
• 17 Years in IT
Agenda

• Context – Security Framework
• Multi Factor Authentication (MFA)
• Protecting your cloud workloads
• Protecting your users
Security Framework
Our Approach

Policy Framework
Regulations and incident handling process

Technology
Software, devices and tools

Education
Keep users up-to-date and vigilant
Security Policies
Application Patching
Security Education
Preventative Scanning

Prevention

Policy Management

Application Patching

Data Security

ACL

Our Brand

ACL

Encryption

MFA Encryption

FW/IPS

Encryption

IPS/IDS

Encryption

Email Security

VPN

Network Security

End-Point Security

Network Security

Perimeter Security

Security Policies

Preventative Scanning

Security Education

Application Patching

Our Brand
Traditional/Pre-COVID
Post-COVID
Multi Factor Authentication
Who can access your data?

- Access control
- Password policies
- Multi Factor Authentication
Protecting your cloud workloads
Cloud Solutions

- Vulnerability Scanning
- Application Protection
- Workload Protection
- Compliance
  - AWS CloudTrail
  - Cloud One Conformity
Technology
Datacenter and Automation
In Practice!

- Example of automated reports for cloud security compliance

Hi Team,
There are some instance in AWS required your action!!

DSA Not Install (4)

<table>
<thead>
<tr>
<th>AWS ID</th>
<th>Region</th>
<th>Instance ID (Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>827099252238</td>
<td>us-east-1</td>
<td>'l-0ebde1e00e9b0ab6c (linux target)</td>
</tr>
<tr>
<td>827099252238</td>
<td>us-east-1</td>
<td>'l-04fb765b36d2f14cf (windows target)</td>
</tr>
<tr>
<td>827099252238</td>
<td>us-east-2</td>
<td>'l-0a7369f4888a0d5f1 (AWX-Ansible-Ohio)</td>
</tr>
<tr>
<td>827099252238</td>
<td>us-east-2</td>
<td>'l-002e33d5fd24d8ce3 (AWX-ELB-Controlled)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Public Read</th>
<th>Public Write</th>
<th>Public Read ACL</th>
<th>Public Write ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>product-experience-attack-platform</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

low the list of port scan we have found as of **20201126-0244**.

<table>
<thead>
<tr>
<th>Region</th>
<th>Instance ID</th>
<th>Instance State</th>
<th>Public IP</th>
<th>Open Port</th>
<th>Issue</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-2</td>
<td>i-0a7369f4888a0d5f1</td>
<td>running</td>
<td>3.139.109.232</td>
<td>3389</td>
<td>Open RDP Service</td>
<td>Restrict port to trusted IP range</td>
</tr>
</tbody>
</table>
Protecting your users
User - Challenges

• Enabling remote updates
• Controlling/Blocking unwanted applications
• Blocking USB
• User education + training
### Application Control

![Trend Micro Apex Central](image)

#### Log Query

<table>
<thead>
<tr>
<th>Generated</th>
<th>User Name</th>
<th>Endpoint</th>
<th>File</th>
<th>Action</th>
<th>Policy</th>
<th>Criteria</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/05/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer_Setup14.5.1691.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>6d13b23754d00e34810672ea8094...</td>
</tr>
<tr>
<td>09/04/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer_Service.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>558562b6a149a486e27511408595f5...</td>
</tr>
<tr>
<td>09/04/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer_Service.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>558562b6a149a486e27511408595f5...</td>
</tr>
<tr>
<td>09/04/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>eda5ef295b25d14b7c5e91a03755...</td>
</tr>
<tr>
<td>09/04/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>eda5ef295b25d14b7c5e91a03755...</td>
</tr>
<tr>
<td>09/04/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>eda5ef295b25d14b7c5e91a03755...</td>
</tr>
<tr>
<td>09/04/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>eda5ef295b25d14b7c5e91a03755...</td>
</tr>
<tr>
<td>09/04/2019</td>
<td>NT AUTHORITY\SYSTEM</td>
<td>IE-0021</td>
<td>TeamViewer.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_CSSS_RemoteControl</td>
<td>eda5ef295b25d14b7c5e91a03755...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
<tr>
<td>09/03/2019</td>
<td>TREND Micro</td>
<td>DE-0001</td>
<td>USBDev.exe</td>
<td>Blocked</td>
<td>EU_Baseline_20190830</td>
<td>EU_Cert_NitSoft</td>
<td>0a95944773b0ba13232c0cb930a4f...</td>
</tr>
</tbody>
</table>

© 2020 Trend Micro Inc.
Credential Theft

• 1 in every 99 emails is a Phishing attack 🐠
• Office 365 Phishing is the most common 🔥
• Office 365 is the one that puts our domain credentials at most risk 😱
Tackling Phishing

1. Monitoring the latest phishing lures and social engineering techniques

2. Mirroring these techniques through simulations

3. Follow up training modules from Phish Insight F2F/Zoom Sessions

4. Security Awareness Campaigns
   - We’ll get to Poppulo in a bit....
The Future of Cyber Security Awareness is here... and it's FREE!

Would your employees fall for a phishing scam?
Help prepare your employees for real phishing attacks.

Try It Now for Free