10 tips for building secure Private PaaS clouds

Introduction

The following list has been composed based on AVET INS experience gained during auditing, pen-testing and designing secure Private PaaS clouds. We tried to write our tips in such way that they can be applied to any Private PaaS cloud platform. Those tips under no circumstances are a comprehensive control list and it was not our objective to provide such list. While some remarks can be applied to public or community PaaS/SaaS/IaaS solutions they were not our target.

We plan to update this document periodically to address new issues and problems as cloud computing and therefore related threats and vulnerabilities evolve.

10 tips

1. **Deploy security policy that address cloud security issues.**
   If security policy is already in place assure that it addresses cloud issues as well (like administration procedures for example or access control). If your cloud deployment is based on virtualization assure that your virtualization solution has been address in security policy as well. Update your security policy, guidelines and procedures appropriately.

2. **Perform threat modeling** for applications and services that will be hosted in your cloud.

3. **Identify hardware and rooms** that will be used for your cloud deployment. Make sure that you always have up-to-date list of those assets.

4. **Address physical security issues** related to rooms and hardware hosting your cloud. Make sure that appropriate approach to this area has been address in your security policy. Update documentation if needed.

5. **Build and provide both test and production environment**. Enforce proper separation of those environments.

6. **Secure access to administrative and applications interfaces.**

   - Change all default/installation/deployment time passwords immediately.
   - Disable anonymous / public access where and when possible.
   - Secure access to virtualization interface (if virtualization is being used).
   - Secure access to operating platforms.
   - Secure access to databases and their interfaces. If possible disable remote database network access. If your database is using stored procedures be sure to remove unneeded procedures and that proper access rights has been assigned to those left.

- Secure access to applications.
- Firewall all network services.
- Deploy IPS to monitor cloud network traffic and block attacks.

7. If your cloud platform offers some form of **compartmentalization / separation** for running applications enable it.

8. If your cloud platforms offers some form of **internal encryption** enable it.

   - Enable strong encryption for remote administration interfaces.
   - Enable strong encryption for swap memory.
   - Enable strong encryption for internal cloud services. If this is not possible, use IPSEC or SSL tunnels.

9. **Patch Management** – patch your cloud services and applications and operating platforms (stacks) accordingly.

10. **Test and audit** your cloud infrastructure periodically. **Monitor** it constantly. Enable appropriate logging functionality not only to help monitoring process but also to support incident management.