SECURITY DYNAMICS – ADAPTATION OF ICT INFRASTRUCTURE TO CLOUD COMPUTING – THREADS AND OPPORTUNITIES

Willian Dimitrov[1], Galia Novakova Nedeltcheva[2]
[1]University of Library Studies and IT, Department of Computer Science
119 "Tsarigradsko shose" Bul., 1784 Sofia, Bulgaria

[2]Sofia University, Faculty of Mathematics and Informatics
5 James Boutchier Str., 1164 Sofia, Bulgaria
r.nikolov@unibit.bg, galianovak@gmail.com

Abstract: *The adoption of new technologies in organizations requires a preliminary assessment of risks, pro and cons of the planned change (SWOT analysis and change management). This paper acknowledges the important changes which are occurring in the security of the ICT systems in the organizations as a consequence from the transfer to the cloud services.*

Traditionally, IT is positioned behind the firewall of any organization and all servers, virtualized or not, are specific as a service for any business. The authority which supports the security systems could choose the components for security among multiple proved products – firewalls, antivirus systems, servers, updates management, proxy servers, etc. In this way is guaranteed the high level of control upon the security of IT environment and the requirements of different standards for security.

Keywords: SECURITY, ICT INFRASTRUCTURE, CLOUD COMPUTING, DYNAMICS

1. Introduction

In the Cloud infrastructure the servers are virtual and are shared between different organizations with different kind of business. In case, the team of an organization is necessary to get together all resources from a public cloud, which is located in Singapore for instance, with the private cloud located in England, then the team could not make use of proved and matured products on the market in order to guarantee the security of the connection. This could lead to reduced trust in the security of Cloud environment [3].

2. Adoption of ICT infrastructure to Cloud Computing

In this section we discuss an example of an organization that has a well developed security of ICT system and it includes well subsystems for:

- application of updates of all operational systems (OS), applications, network devices, printers, and UPSs;
- assets management, taking into account all platforms with details for the hardware, installed software and its utilization.

With the invent of Cloud computing the requirements to the functions of the above mentioned subsystems are changing. In this case, the architecture is based on two or more distant data centers and hypervisors with virtual machines (VM) in them. The VM could be on, off or in snapshot mode.

The subsystem for updates has to keep track of all VMs from all data centers of the provider and to influence on them, because when one VM is moved from one data center to another it could be left without update. The process of update has to be linked with the subsystem of the asset management as in the subsequent need for update all VM machines that are stopped and the ones in snapshot mode will be missed.

We feel that the subsystem for asset management, combined with a function for monitoring of VM dynamics and in compliance with the cloud infrastructure, can be the second pylon after the updates, on which to base overall scheme for security management of the VMs.

In Table 1 below are presented the basic processes which are leading to new requirements for updates and monitoring of the security of VMs in the dynamics, typical for their life-cycle in Cloud environment.

Table 1. *Basic processes leading to new requirements for updates and monitoring*

Term	Process	Description
On/Off	Some VM stop and start many times in a short period.	The virtual machine is created, used and destroyed before it is checked and updated [5]
Snapshot Rollback	Rollback	The return of the virtual machine from the pre-stored image in a previous condition can lead to non updated versions of one or more applications [5]
VM Migration	Transfer of virtual machine	The virtual machine is copied, without being stopped or at a standstill, in another data center infrastructure provider of cloud services. It is related to a change in the DNS and other problems.

The Reflection of Elasticity

Key difference between Cloud computing and conventional data centers is the elasticity. It is essentially a key character of virtualization. Servers are as file and executable tasks, and may be subject to various operations – copy, moving, resize of the elements of the OS, disk space, number of network controllers, snapshots, reserved templates with the aim of next backup.

The elasticity gives possibility of the organizations to multiply the servers: their number is growing quickly as well as the available power for computing. This increases the risks of compromise since:

- When coping the server all its undiscovered and exposed vulnerabilities are also duplicated;
- Coping the servers is dramatically increasing the total area for attacks in the data center.

The non-active images of servers as well as the snapshots are VMs which saved in files and are intended for subsequent reactivation or serve as templates for new servers. This advantage is at the expense of security: as these machines are not active when installing security fixes, they remain unprotected from newly discovered vulnerabilities, without configuration changes with changes in policies and does not reflect the change of access rights for the users [6].

An incorrectly configured server can be replicated in cloning of new servers and to become an outbreak of the entire server farm of the supplier. The elasticity involves security issues that do not exist in traditional data centers.

It becomes necessary functions of monitoring security, which include:

- AAA control that manages who may request additional resources from pools of shared resources or to release used resources;
- Monitor and audit requests to obtain and release resources to ensure that quotas are met and services remain available;
- Providing guaranteed deletion of residual data from all components of the pool with consumed by the tenant resources.

From the perspective of the tenant it is necessary to have a sense of infinite capacity resource. From the perspective of the provider of cloud services he owns a pool of fixed size that contains shared between tenants' resources and must be managed so that the conditions for quality of the service are met [8].

Ready Virtual Machines (VM)

In recent years, all manufacturers of devices for protection - firewalls - IDS /IPS, UTM, anti-spam devices, antivirus devices started to offer ready-made virtual machines [1] to test their products and real application environments virtualization. Separately, there are many small and big manufacturers of ready virtual machines that can be copied from the Internet and to be applied directly to virtualization environments.

Large manufacturers offer tools to prepare their own VM and virtualization of existing production platforms on real hardware to be transferred in an environment of hypervisor for a variety of reasons, such as increasing trend for hardware problems [7].

The production of VMs with ready-installed applications and their marketing brings threats that in our opinion are in most cases similar threats from uncontrolled copying of software from Internet sites and installing it on the office computers.

Initially, ready VMs were designed for traditional data centers with server for virtualization, but today the focus of their application moves into cloud computing [2],[3]. What effects might cause this?

In the environment of the provider of cloud services may fall machine that is compromised or such that is prepared and provides tools for implementing the attacks of various types. Publications on the subject are mentioning possibilities to implement the tools bot-net, DLP, DdoS, theft of encryption keys [4].

What could be the approach to this threat? For example, such as applications for virus detection on the images of VMs that are offline or testing in isolated mode.

As well, it would be very much useful if we have an asset management which may keep in dynamics the report on all VMs together with the applications on them and even their licenses, regardless how long they have existed.

3. Securing Internet of Things (IoT) Devices

The coexistence of many tenants in a cloud environment is another aspect of the security of virtual machines. Joint persistence of virtual machines that are owned by different tenants in a cloud environment poses a range of risks which is our next research direction to explore.

Nowadays Internet of Things (IoT) is a natural extent of conventional ICT. It comes with BYOD and many smart devices and the big data. The staff takes care after installation of the smart devices, WSN, IoT middleware and the cloud services are not proved for security. All this extend the surface for attack.

IoT manufacturers use cheap components and boards for the most parts which lack the power or capability to run fundamental security features, such as anti-malware, anti-virus, firewalls and encryption. These devices are thus left not only vulnerable, but worst, making them virtually impossible to secure. As for the IoT devices, the direction towards solving this security threat will require a combined effort from consumers, manufacturers and technicians.

IoT connected devices should always exist behind a Firewall. Moreover, the default firewall settings and passwords of many WiFi routers and devices are not adequate to block such traffic. Usually, it is not the case that the end users could hire an expert to audit the home or office network security. By 2020, it is estimated that the number of connected devices is expected to grow exponentially to 50 billion.

To address the security issues at the manufacturing level of IoT devices, there needs to be strict security standards and regulations put in place. This however, is a huge effort. Meanwhile, many IoT devices will become obsolete or even be returned. With newer versions being released, manufacturers have more opportunity to built-in security. Security staff should investigate and compare solutions which focus on protecting all on-premise devices, for example gateways with embeded firewalls which add a layer of protection in front of IoT devices. This is extremely important because, as mentioned, IoT devices often have limited computing resources and for the most parts are unable to manage their own security on-board.

Incorporating security into the design of components used in the IoT is essential for securing the operations of the IoT and the cyberphysical infrastructure upon which society depends. The penetration of IoT and its part in the critical infrastructure requires incorporating security into the design of components. Given the increasing functionality, interconnectedness and use of the IoT within critical infrastructure, securing the integrity of command and control within the IoT is essential.

There are several challenges to incorporating security into the design of IoT components. These challenges are as follows: (1) precisely describing confidentiality and integrity policies in ways that are amenable to formal reasoning, (2) maintaining logical consistency among confidentiality and integrity policies and implementation at all levels of abstraction, from high-level behavioral descriptions at the user level, down to implementations at the level of state machines and transition systems, (3) Incorporating confidentiality and integrity policies into current design flows, and (4) providing certifiers with compelling evidence of security that they can quickly and easily reproduce and verify for correctness.

Together with IoT invasion there are existing already installed automated systems such as: Building Automation Systems (BMS), Industrial Control Systems (ICS) and SCADA. IoT would coexist with such kind of systems in synergy and would add smart properties to those kind of systems.

This would lead to new extend of attack surface. Potentially vulnerable existing BMS are now prevalent in many buildings and offices, including hospitals, airports, sports stadiums and government departments. The environments of these organisations are therefore vulnerable to outside control; control that has the potential to impact external and internal communications, computer networks, building access, lighting and heating. Downtime on every single system has a direct influence to the wellbeing of people, the performance of businesses and the corporate reputation of organisations, institutions and entire industries. Would a hospital with no lighting be able to treat patients? Could an airport function without communications for a whole day? How would a business operate if its staff could not access its building? Such attacks, even if quickly resolved, could cause untold damage in fragile systems that rely on continued operation, such as electricity generators, casinos, hospitals or stock exchanges, to name a few. Organisations would cease to function and potentially collapse, taking down their reputation as well as severely inhibiting their commercial performance. There are multiple reasons behind such attacks (See Table 2) as follows:

- Activist groups wanting to break up organisations they take issue with
- Terrorists wanting to disrupt national functions, for example transport or government operations
- Nation states wanting to harm organisations they consider a competitive risk or a threat to their security
- Companies wishing to sabotage competitors
- Aggrieved former employees wanting revenge
- 'The bored teenager' testing his hacking skills.

If those actors gain control of BMS, the damage that can be done is highly significant [9]:

Table 2. *Impact of compromise to the system [9]*

System	Impact of compromise
Management System/ Dashboard	Lockout genuine users from system
Lighting	• Deactivation of lights may cause safety and productivity issues including public panic and inability to conduct business as usual • Flickering of lights could cause health issues • Increased situational awareness for criminals by activating lighting remotely • Reduces situational awareness for guards/ CCTV operator by deactivating lighting remotely
Access Control	• Remote release of secure doors resulting in unauthorised access • Deactivation of door release to inconvenience users/force use of green break glass • Deactivation of authorised users • Addition of unauthorised users • Erasure of access logs to cover criminal activity
HVAC	• Deactivation of cooling to cause plant/ ICT equipment to overheat/shutdown/ malfunction • Activation of heating to cause plant/ ICT equipment to overheat/shutdown/ malfunction • Deactivation of cooling/heating making normal working difficult or sometimes impossible
CCTV	• Increased situational awareness for intruder to be able to see guard locations and blindspots • Ability to turn cameras away from criminal activity • Ability for intruder to erase footage • Ability to capture sensitive information such as passwords, sensitive business details or private activity that could cause embarrassment if made public
Lifts	• Denial of service • Override lift access control
Tenant Billing	• Tenant's under or overcharged for utility usage, affecting profitability or alienating customers
Building Information Modelling and CAD	• Criminals have a greater awareness of where key systems are located and how they are connected and powered
Building/ Perimeter Intruder Detection System	• Deactivation of system allowing unauthorised access • Creating false alarms for distraction • Erasure of event records to hide criminal activity
Fire Detection	• Cause panic and disruption by activating alarm or risk lives by deactivating it (Note: We assume that fire detection would not be under the control of the BMS to comply with standards therefore vulnerabilities should be limited, but this may change in future)

The threats from IoT increases by a number of factors (see also Fig.1):

- The number of connected "things" anticipates the possibility to be controlled, monitored and organized;
- Many devices have little or no any built security;
- There is no any standard procedure for securing the devices for Internet of Things, even there are no any best practices;
- An increasing number of devices provide access to personal information;
- Demand for business opportunities with this class of devices and systems will continue to be a higher priority than their security.
- Connecting plain old automation systems that are designed without security in the requirements to IoT. Devices that were never built up for security are increasingly becoming connected to networks, and so becoming hackable.

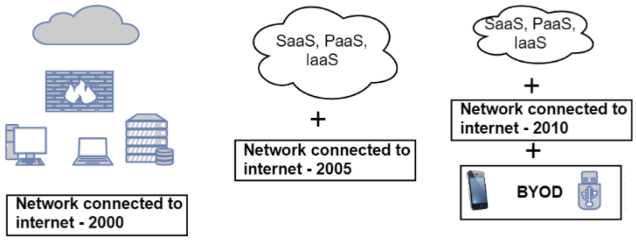
Network connected to internet - 2000
SaaS, PaaS, IaaS
+
Network connected to internet - 2005
SaaS, PaaS, IaaS
+
Network connected to internet - 2010
+
BYOD

Fig. 1. *Growing threat landscape factors from 2000 to 2010*

The challenge are the above mentioned unconnected areas: asset/ facility management and IT. But, as more BMS become connected, the more departments need to work closely together, or facilities managers need to become security experts. See Fig. 2 below.

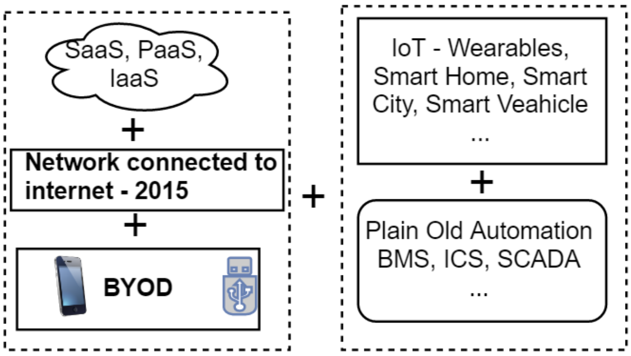
SaaS, PaaS, IaaS
+
Network connected to internet - 2015
+
BYOD
+
IoT - Wearables, Smart Home, Smart City, Smart Veahicle ...
+
Plain Old Automation BMS, ICS, SCADA ...

Fig. 2. *Extension of threat surface after 2015 with IoT and old automation system*

3. Conclusion

In the present paper the attention is on the main aspect of the above mentioned new level of synergy between Cloud and IoT concerning security, taking into account that this is a new ecosystem of business relations. So, the paper through light on trends of security risks that are hidden in this kind of supply chain.

References

[1] Build a virtual appliance. How to Build a Virtual Appliance, http://www.vmware.com/appliances/getting-started/build/how/:Accesed 18.09.2012, 2012.

[2] BitNami Carlos. How to start a bitnami machine image (ami)? http://wiki.bitnami.org/cloud/How_to_start_a_BitNami_Machine_Image_(AMI)%3f, December 2011.

[3] Intel IT center. What's holding back the cloud? In Intel Survey on Increasing IT Professionals Confidence in Cloud Security. Intel Corporation., May 2012.

[4] Claudia Eckert. Cloud computing new challenges for it security. In Fraunhofer Institute for Secure Information Technology (SIT), February 2010.

[5] RAPID7 Corporate Headquarters. The dynamic nature of virtualization security. In The need for real-time vulnerability management and risk assessment, 2012.

[6] Intelligence and National Security Alliance. Risks and benefits of cloud computing for the intelligence community. http://insaonline.com/assets/files/Press%20Releases/RisksAndBenefitsofCloudComputingfortheIC.pdf, March 2012.

[7] Transworld Data Research. Transworld data case study. In Building Workload Images for IBM System z with SUSE Studio, 2012.

[8] Deb Shinder. http://www.windowsecurity.com/articles/security-considerations-cloud-computing-part5.html. Security Considerations for Cloud Computing (Part 5) - Rapid Elasticity, June 2012.

[9] Andrew Kelly, QinetiQ Cyber Consulting team, Building Management Systems: the cyber security blind spot, 2015, https://www.qinetiq.com/services-products/cyber/Pages/bms-the-cyber-security-blind-spot.aspx#