International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1605

(03/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security design

Security requirements of public Infrastructure as a Service (IaaS) in cloud computing

Recommendation ITU-T X.1605

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	**X.1602–X.1639**
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	X.1700–X.1729

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1605

Security requirements of public Infrastructure as a Service (IaaS) in cloud computing

Summary

Infrastructure as a Service (IaaS) platforms and virtualized services face different, and perhaps more, challenges and threats than traditional information technology infrastructure and application. IaaS platforms that share computing, storage and networking services need protections specific to threats in an IaaS environment. Recommendation ITU-T X.1605 documents security requirements of public IaaS in order to help IaaS providers to improve security of the IaaS platform throughout the planning, building and operating stages.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1605	2020-03-26	17	11.1002/1000/14094

Keywords

Cloud computing, IaaS, security requirement, virtual resources.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1605

Security requirements of public Infrastructure as a Service (IaaS) in cloud computing

1 Scope

This Recommendation analyses security challenges faced by Infrastructure as a Service (IaaS) providers in IaaS environments, and specifies security requirements of public IaaS in cloud computing. This Recommendation is applicable for public IaaS providers.

This is a high-level description of the security requirements of IaaS implementation. Detailed implementation guidance is out of scope for this document.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1642]	Recommendation ITU-T X.1642 (2016), *Guidelines for the operational security of cloud computing*.
[ITU-T Y.3502]	Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.
[ITU-T Y.3513]	Recommendation ITU-T Y.3513 (2014), *Cloud computing – Functional requirements of Infrastructure as a Service*.
[ISO/IEC 27002]	ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.
[ISO/IEC 27031]	ISO/IEC 27031:2011, *Information technology –Security techniques– Guidelines for information and communication technology readiness for business continuity*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer (CSC) [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.4 cloud service partner [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.5 cloud service provider (CSP) [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.6 Infrastructure as a Service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

3.1.7 security challenge [b-ITU-T X.1601]: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats.

3.1.8 vulnerability [b-NIST-SP-800-30]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
API	Application Programming Interface
BIA	Business Impact Analysis
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DRO	Disaster Recovery Object
DSP	Digital Service Provider
IAM	Identity and Access Management
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IdM	Identity Management
I/O	Input/Output
NIC	Network Interface Card
OS	Operating System
OTT	Over The Top
PaaS	Platform as a Service
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SaaS	Software as a Service
SLA	Service Level Agreement
SQL	Structured Query Language
VDC	Virtual Data Centre

VLAN	Virtual Local Area Network
VM	Virtual Machine
VXLAN	Virtual Extensible Local Area Network
XSS	Cross Site Script

5 Conventions

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In this Recommendation and its appendices, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview

Infrastructure as a Service (IaaS) is a category of cloud services, in which the cloud capabilities type provided to the cloud service customer (CSC) is an infrastructure capabilities type [b-ITU-T Y.3500]. IaaS allows CSCs to use cloud infrastructure resources (computing, storage or networking) which can be rapidly provisioned and released with minimal management efforts. Public IaaS services enable CSCs to launch their business quickly and easily without establishing new information and communication technology (ICT) infrastructure, and CSCs can use these resources to develop, host and run services and applications on-demand in a flexible manner elastically as needed.

Based on the layering framework developed together with ISO/IEC as defined in [ITU-T Y.3502] and the high-level concept of IaaS defined in [ITU-T Y.3513], high level concept of IaaS security requirements is illustrated in Figure 6-1.

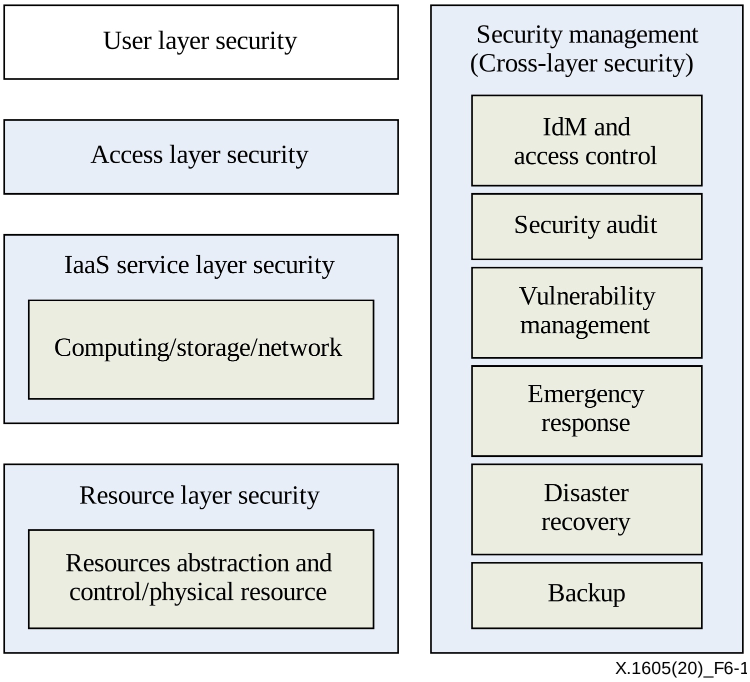

Figure 6-1 – High-level concept of IaaS security requirements

The user layer is the user interface through which a CSC interacts with the cloud service provider (CSP). The functional components of the user layer include user function, business function and administrator function, which interact with cloud services provided by CSP, perform CSC related administrative activities and monitor cloud services. According to the responsibilities between CSP and CSC, CSCs should take charge of security mechanisms of the user layer because they usually use their own tools or systems to access the IaaS service. If otherwise, the tools or systems of the user layer are provided by CSP, CSP should provide the tools or systems that meet the best practice of industry for security. Security requirements of the user layer are out of the scope of this Recommendation.

The access layer provides a common interface for both manual and automated access to the capabilities available in the service layer. The functional components of access layer include access control and connection management. The access layer is responsible for presenting IaaS service capabilities over one or more access mechanisms such as web and application programming interfaces (APIs). The security requirements of access layer are defined in clause 8.

The service layer contains the implementation of the IaaS services provided by CSP. It contains and controls the software components that implement the IaaS services, and arranges to offer the services to CSC via the access layer. The security requirements of the service layer are defined in clause 9.

The resource layer components include resource abstraction and control, and physical resources as defined in [ITU-T Y.3502]. The virtualized resources are generated and controlled through software abstraction. The security requirements of the resource layer are defined in clause 10.

Security management provides fundamental cross-layer security management capabilities, which are implemented throughout the user layer, access layer, service layer and resource layer as described above. The security management requirements of identity management and access control, security audit, vulnerability management, emergency response, disaster recovery and backup are defined in clause 11.

7 Security challenges for the IaaS environment

Due to the vast advantages of IaaS, IaaS has become one of the most important services of CSPs especially for traditional telecom operators, over the tops (OTTs) and digital service providers (DSPs), and has gained a rapid expansion. Along with the fast IaaS development, security issues remain a major and important concern that cannot be ignored. IaaS platforms and services are facing more challenges and threats than traditional information technology infrastructure and application, especially due to wide implementation of virtualization technologies, shared resources for multi-tenants, among others.

Since a public IaaS could have many co-existing CSCs from many different organizations, both security and privacy protection are the most important factors when CSCs evaluate the choice of public IaaS services.

In brief, the security challenges that a public IaaS faces may come from the following aspects:

1) Virtualization: As an important technical feature of cloud computing, virtualization technology enables different virtual machines (VMs) to run on one same hypervisor, but it also makes files contained in VMs vulnerable to be illegally modified. Furthermore, once the vulnerabilities of the hypervisor are exploited, all the VMs running on it would face the same security risks. These risks be caused by:
   - Inappropriate configuration and network isolation of physical hosts. Attackers could directly make use of the vulnerabilities of the hypervisor.
   - Vulnerabilities of interfaces between the VMs and the hypervisor. Attackers could exploit the vulnerabilities to control the hypervisor; this is called VM escape.
2) Open APIs: As a premise of managing VMs automatically, open APIs could enlarge the attacking surface by abusing or exploiting vulnerabilities such as lack of authentication, authorization or integrity check, which would destroy many applications.
3) Network and Internet connectivity: Network threats such as distributed denial of service (DDoS) attack, man-in-the-middle attack, IP spoofing attack, etc., could be launched not only from the traditional network, but might also emerge from VMs in the same host machine, which is much more difficult to defend within the vague boundary environment of a virtualized network.
4) High degree of resource sharing: This technical feature might provide a more specific target. If the physical host machine or the physical network were destroyed, all of their VMs would be impacted. The disposal of retired or replaced storage devices relates to the confidentiality of all CSCs' data. It would also bring more isolation difficulty between different CSCs. If the isolation of different VMs is not configured properly, the possibility of data leakage or even network attacks between different VMs may increase significantly. Any accidents that occur would result in significant security risk and consequences.
5) Scalability of virtual resources: The elastic expansion of virtual resources and the dynamic adjustment of a virtual network's security perimeter introduce the fast growth of east-west network flow and new complex security demands. It requires that security facilities should be agile and be able to work collaboratively, but most security equipment and systems function individually, which is a lack of a mechanism for effective cooperation.
6) Configuration management: Cloud computing environment contains various types and huge amount of assets, and different service types, which introduce a high demand of configuration including access control, isolation and data backup, etc. Improper configuration may expose new attack surface, or even leak sensitive information directly.
7) Logging issues: Various log data of operating systems, applications and security equipment can help operators avoid disasters in advance, and even detect the root cause of security incidents. In the cloud computing environment, log acquisition, protection and time

synchronization become more complex. For example, the omission of log protection would bring the risk of tampering, while the lack of time synchronization would make it difficult to correlate heterogeneous logs.

8 Security requirements of the IaaS access layer

The access layer of IaaS is responsible for presenting IaaS service capabilities for CSCs to access and manage over one or more access mechanisms. The access mechanisms include, but are not limited to, the following:

– Web access

– API access.

Another responsibility of the access layer is to implement appropriate connection management mechanisms to provide enforcement of QoS policies, load balance and secure transmission regarding the traffic and connections from and/or to the user layer functional components.

8.1 Security requirements for web access

1) IaaS CSP is required to apply authentication and authorization measures for CSC to access the IaaS service with web access, such as authenticating the request through the CSC's credentials and validating the authorization of the CSC.

2) IaaS CSP is required to apply an access control mechanism for CSC to use related service capabilities.

3) It is recommended that IaaS CSP provides a secure communication tunnel for CSC via web access.

4) It is recommended that IaaS CSP provides web access protection for CSC, such as validity checking for input and output, checking for request integrity, defence capacities against web intrusion behaviours, such as structured query language (SQL) injection, cross site script (XSS), remote command execution, etc.

5) IaaS CSP is required to support untampered logging, analysis and security auditing capabilities for web access behaviours.

8.2 Security requirements for API access

1) IaaS CSP is required to support authentication and the authentication of user credentials for CSC when calling the service API, such as signing on to the API to ensure that only legitimate callers are used.

2) IaaS CSP is required to provide an access control mechanism for CSC when calling the service API.

3) It is recommended that IaaS CSP provides a secure communication tunnel for CSC via API access.

4) It is recommended that IaaS CSP provides API interface protection for CSC, such as checking for request integrity, defence capacities against attack behaviours such as replay attack, code injection, etc.

5) IaaS CSP is required to support logging, analysis and security auditing capabilities for API calling behaviour.

9 Security requirements of the IaaS service layer

The service layer of IaaS contains the implementation of the services provided by CSP. The service layer contains and controls the software components that implement the IaaS services (such as computing service, networking service, storage service, etc.), and arranges to offer these IaaS services to CSCs via the access layer.

9.1 Security requirements for computing service

1) IaaS CSP is required to provide isolation mechanisms for virtual resources including the isolation of the central processing unit (CPU), internal network, memory and storage, etc., and only permit communications that meet the security policy among different virtual resource units, such as VMs.

2) IaaS CSP is required to support the setting of resource upper limit for a single virtual resource unit in a physical host, which would avoid degradation of performance caused by a specific virtual resource unit's excessive occupation.

3) It is recommended that IaaS CSP supports the automatic migration of the virtual resource unit if the hosted server fails, which would prevent the interruption of services running in the virtual resource.

4) IaaS CSP is required to support integrity check of the virtual resource unit's images to prevent malicious tampering, and ensure that a logical volume can be mounted only by one virtual resource unit simultaneously.

5) IaaS CSP is required to support the migration of security policy, which would be simultaneously synchronised with the virtual resources unit accordingly.

6) IaaS CSP is required to provide the CSC administrator with the capability of customizing the security policy among virtual resource units.

7) IaaS CSP is required to provide the CSC with the capability of complete deletion of their own data. Once a virtual resource unit is removed by the CSC, the image files, snapshots and backups should also be simultaneously erased.

9.2 Security requirements for storage service

1) It is recommended that IaaS CSP supports a data redundancy mechanism. CSCs' data should be guaranteed no less than two backups in different physical locations and the mechanism should be transparent to CSCs.

2) It is recommended that IaaS CSP supports concurrent input/output (I/O) control and safe parallel access for multiple VMs using the same storage system.

3) IaaS CSP is required to guarantee the access control of stored data that could be executed both on the logical and physical storage entities, which should not be bypassed by any change in the physical location of storage.

4) IaaS CSP is required to guarantee CSCs' that data can be completely erased, including:

   – Complete data erasure should be performed before the storage resource is reassigned to a new CSC.

   – Once a CSC's files/object are deleted, the corresponding storage area in the physical volume should be rightly overwritten or labelled as write only, avoiding unauthorized recovery.

   – Once a CSC's data is migrated, the CSC's metadata is required to be completely erased immediately.

9.3 Security requirements for networking service

1) It is recommended that IaaS CSP provides the CSC with the capability to monitor the north-south, east-west network traffic of their own virtual resources.

2) It is recommended that IaaS CSP provides the CSC with the capability to implement the network interface bandwidth-control of virtual resources.

3) IaaS CSP is required to provide isolation measures between the CSCs' virtualized network and IaaS platform and management network, such as forbidding CSC accessing the host machine or management node.

4) IaaS CSP is required to implement network access control list (ACL) mechanism to achieve security isolation and access control within the virtualized networks.

5) It is recommended that IaaS CSP supports defending against network attacks such as virtual local area network (VLAN) or virtual extensible local area (VXLAN) hopping.

10 Security requirements of the IaaS resource layer

According to the functional components of IaaS resource layer, security requirements of IaaS resource layer include:

– security requirements for resource abstraction and control; and

– security requirements for physical resources.

10.1 Security requirements for resource abstraction and control

The resource abstraction and control functional component enables CSPs to offer qualities such as rapid elasticity, resource pooling and on-demand self-service. It includes the virtual resource pool (such as, virtual computing resource, virtual network resource, etc.), and virtual resource management platform. The security requirements for resource abstraction and control will be illustrated from the perspective of virtual resource provision and management.

10.1.1 Security requirements for virtual resource pool

10.1.1.1 Security requirements for virtual computing resource

1) The virtual computing resource units (such as virtual machine, container, etc.) are required to be isolated logically with each other.

2) It is required that the virtual computing resource unit cannot be influenced by other units or host machines when encountering abnormal accidents or failure.

3) It is required that the virtual computing resource unit cannot be used beyond its quota.

4) "Copy", "paste" and other commands are recommended to be forbidden between different virtual computing resource units, or the host machines.

5) It is recommended that IaaS CSP supports the real-time monitoring of virtual resources through in-band or out-of-band mode, and send alarms once abnormalities are detected. For each virtual resource unit, the monitored objects should include the running status, resource consumption and migration status, etc.

10.1.1.2 Security requirements for virtual network resource

1) CSC's virtual network is required to be isolated logically from each other by implementing the measures of VLAN, VXLAN, ACLs, etc.

2) A monitoring capability of network traffic is required to be provided between different virtual resource units.

3) A bit rate control capability is required to be provided over virtual ports.

4) It is recommended that network attack behaviours (such as IP spoofing, worms, etc.), originated inside the virtual resources can be detected and prevented.

5) The promiscuous mode of the virtual network interface card (NIC) ports is required to be forbidden to prevent sniffing of network traffic.

10.1.1.3 Security requirements for virtual storage resource

1) The virtual storage resource pool is required to be isolated between different CSCs.

2) The security measures over stored data is required to be executed both on logical and physical storage entities.

3) The direct access to physical storage resources is required to be forbidden.

4) The capability of concurrent I/O control and safe parallel access is required to support for multiple virtual resource units that using the same storage entities.

5) It is recommended that the virtual storage resources can support elastic expansion without interrupting the normal storage services.

10.1.2 Security requirements for virtual resource management platform

1) The access control measures are required to be implemented appropriately to prevent illegal access to the virtual resource management platform.

2) It is recommended that only the necessary components and applications are installed and irrelevant service ports are closed, to follow the principle of risk minimization.

3) It is required that the attacking behaviours upon the virtual resource management platform can be detected and alarmed timely, and the logs should be recorded including the source IP address, attacking type, time stamp, etc.

4) The real-time monitoring capability over the virtual resources is required to be provided, including running status, resource occupation, migration, etc.

5) It is recommended that the unnecessary and idle virtual resources can be disabled.

6) The management commands over virtual resource management platform are required to be transmitted in a secure tunnel.

7) It is recommended that the privileged commands can be restrained when they are remotely executed.

8) It is required that the illegal virtual resource units can be isolated and disposed of appropriately to minimize the subsequent influence upon the entire virtual resources.

9) The detection and disposing capability of malicious code is required to be provided.

10) It is recommended that the security policy can be migrated following the simultaneous migration of the virtual resource units.

11) Security patches or security reinforcement configuration are required to be implemented timely once the security vulnerability of virtual resource management components (such as hypervisor, container engine, management components, etc.) are detected, and that they be kept up-to-date.

12) Fault management is required to be provided to maintain upper service continuity, that is, the virtual resource units on a failure host machine can be migrated to another host machine in a timely manner.

13) All operations and events over the virtual resource management platform are required to be logged for later trace and audit.

10.2 Security requirement for physical resource

Physical resources include hardware resources, such as computers, network equipment, storage components and other physical computing infrastructure elements, needed by CSP to run and manage the IaaS services offered to CSCs.

10.2.1 Security requirements for the physical environment

The security requirements for the physical environment for IaaS are contained in [ISO/IEC 27002].

10.2.1.1 Security requirements for physical resources

Physical resources include hardware resources, such as physical networking infrastructure, storage devices, host machines, management terminals and other physical infrastructure elements.

1) The fault detection and positioning capability over physical resources (such as networking equipment, host machines, storage devices, etc.) are required to be provided to maintain the availability and reliability of the underlying physical infrastructure.
2) It is recommended that alternation of physical resources can be detected and marked in a timely manner.
3) It is recommended that the data recovery capability can be provided when some physical components fail.
4) The IaaS platform's defence capability against DDoS is required to be provided.
5) The infrastructure network is required to be divided into different network security domains, logically isolated from each other.
6) Detection mechanisms of network traffic monitoring and intrusion behaviour are required to be implemented, with protection devices deployed at the network boundary including identity and access management (IAM), IPS, firewall, etc.
7) It is recommended that the outgoing network attack behaviours that initiated from the IaaS resource can be detected and prevented.
8) A detection and disposing capability of malicious code is required to be provided, especially for management terminals, host machines and other application servers.
9) It is required that security policy baseline should be implemented and only the terminals and servers which have satisfied the security policies can access the IaaS platform.
10) All operations and events over the physical resources are required to be logged for later trace and audit.

11 Security management requirements

Security management is responsible for applying security related controls to mitigate the security threats in cloud computing environments. The functional components of security management encompass all the security facilities required to support cloud services.

The functional components of security management include:

- identity management and access control;
- security audit;
- vulnerability management;
- emergency response;
- disaster recovery; and
- backup.

11.1 IdM and access control

The IaaS platform should provide unified identity management (IdM) and access control functions for CSCs and IaaS platform administrators.

1) The identity of CSC in the life cycle is required to be unique in each IaaS service and associated with security audit. The identity of CSC is required to be managed, maintained and protected from unauthorized access, modification, or deletion.
2) The IaaS platform is required to provide password policy management for CSCs, which includes, but is not limitedto:

- It is required to use password complexity policy;
- It is required to use password re-setting period mechanism;
- It is required to use random generation of CSCs' initial key, and the initial key must be modified on first login.

3) It is recommended that IaaS platform supports abnormal detection for CSC's identity and that the alarms can be notified to the related CSCs.

4) IaaS platform is required to support multi-factor authentication for CSCs, and the authentication techniques including but not limited to passwords, digital certificates, IC cards, or biometric validation.

5) It is required to support fine granularity authorization strategy according to CSC and group definition of the resources to access. It is required that IaaS platform protects the confidentiality and integrity of CSCs' authentication credentials.

6) The detailed logs of CSC authentication, authorization and other operations related with IdM are required to be stored for later audit.

7) It is recommended that IaaS platform supports docking with CSCs' IdM system.

8) The role and related privileges of IaaS platform administrator are required to be granted to different accounts.

9) IaaS platform is required to use multi-factor authentication for administrators.

10) IaaS platform is required to use the principle of minimizing authority for administrators.

11) Sensitive data such as authentication data, authorization data, etc., are required to be encrypted in the procedure of storage and transfer.

11.2 Security audit

1) The IaaS platform is required to use various records for security audit. the records include, but not limited to:
   - logging, identity authentication and authorization information of CSCs and IaaS platform administrators;
   - operating and maintaining records over IaaS infrastructure by IaaS platform administrators;
   - operating logs over CSC's resources by IaaS platform administrators;
   - operating logs over CSC's own resources by CSC;
   - operation and maintenance logs during running process of IaaS platform.

2) The IaaS platform is required to implement security mechanisms to protect the various records against tampering.

3) All the network clocks are required to be kept in synchronization within the whole IaaS platform to record access and operation systematically.

4) The security audit records shall include the subjects, objects, time, types, and results of the security event.

5) The inter-CSC audit records are required to be isolated from each other.

6) It is required that CSC can collect and view the audit records related to their own resources.

7) The audit records are required to be securely protected, such as forbidding unauthorized access to audit records, prevention from unexpected deletion, modification, overriding and loss.

8) The retention period of audit records is required to meet the legal compliance and the specific retention requirements of CSCs.

9) It is recommended that IaaS platform supports CSC to use third-party auditing systems or interface to achieve auditing goals within the CSC's responsibilities.

11.3 Vulnerability management

The vulnerabilities of IaaS platform can exist in processes, management, configuration, hardware, software, etc.

1) It is required to record the information of all assets and the versions of the IaaS platform, and update the information regularly.
2) It is required to establish the vulnerability assessment mechanism, in which the objects, frequency and evaluation strategy of vulnerability assessment should be clarified.
3) It is required to carry out vulnerability assessment of all assets of IaaS platform regularly, generate vulnerability assessment reports and make recommendations for vulnerability repair.
4) It is required to manage patch and repair process:
   - It is required to track the security threats and security patches issued by various vendors, determine which patches should be installed in the IaaS platform.
   - It is required to test the security patches before installation to ensure that the patches are compatible with the existing system and application.
   - It is required to create the patch update plan for all components of IaaS platform, carry out the patch installation according to the plan, and create records during the installation.
5) It is required to formulate the security configuration baseline of the IaaS platform and configure the components of the IaaS platform according to the baseline.
6) It is required to carry out security baseline inspection of all assets of IaaS platform regularly, form a baseline inspection report and make recommendations for rectification.
7) It is required to audit the configuration strategy changes of the IaaS platform to verify the correctness, consistency, completeness and effectiveness of each configuration item, and ensure that the configuration changes do not bring new security defects.

11.4 Emergency response

Emergency response considerations for IaaS are in accordance with clause 8.9 of [ITU-T X.1642].

11.5 Disaster recovery

Disaster recovery considerations for IaaS should conform to the existing common regulations of IT technology, such as the standard [ISO/IEC 27031]. However, as a fast growing technology, the disaster recovery of IaaS should also consider:

1) Define disaster recovery objects for each CSC. It is required to initiate a business impact analysis (BIA) to determine the disaster recovery objects of different businesses, which is based on recognition of key components and main security risks on the IaaS platform. The disaster recovery objects can be defined by priorities, RPO/RTO, etc. Different DROs determine the corresponding SLA and the service architecture, including high availability technology cross the remote virtual data centres (VDC), cross-region data backup, etc.
2) Regularly backup systems and data. It is required to support the capability of cross-regional data storage and disaster tolerance. Further, the types of system-level backup and data-level backup should be provided to the tenants of the IaaS platform as well as the corresponding disaster recovery capability, which can help CSPs and CSCs implement failover. For CSCs, they can even backup data to a different CSP regularly, to avoid the risk of a long time termination of a single CSP.

3) Validate the disaster recovery plan regularly. Although the systems and data of CSCs may maintain relatively constant, new security risks might also be introduced by infrastructure updates launched by CSPs. So, disaster recovery drills should be regularly conducted and key information should be recorded including the availability, integrity and the validity of disaster recovery plans, the problems and the corresponding solutions in the process, etc.

4) Regularly assess the risk. To support CSCs' business continuity, CSPs should assess the security risks that may impact on CSCs' business continuity plan, which includes failure of IaaS service, disruption of the network between the CSP and CSC, termination of cloud services, etc., and the results should be informed to the CSCs diligently. Further, the emergency response, disaster recovery plans and activities to support CSCs' business continuity should be notified in advance, and even be adjusted according to the CSCs' requirements.

11.6 Backup

Backup considerations for IaaS are in accordance with clause 8.10 of [ITU-T X.1642].

Bibliography

[b-ITU-T X.1601] Recommendation ITU-T X.1601(2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-NIST 500-291] NIST SP 500-291,2011, *NIST Cloud Computing Standards Roadmap*.

[b-NIST-SP-800-30] NIST Special Publication 800-30, 2012, *Guide for Conducting Risk Assessments*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020