Overview of selected KPN Security Policies

Creation date: Wednesday, December 4, 2019 1:33:53 PM

Selected by: Ruud Leurs

Requirement	**Container segmentation and zoning**
Description	Containers must not be consolidated on the same system (i.e. (virtual) machine) when they differ on zone, DTAP purpose (development, testing, acceptance and production), customer or risk-level. The administrator must classify the risk per group of containers in one particular zone and for one customer on the effects of: - kernel panics, i.e. focus on the business continuity aspects. - container break-out and information security, i.e. ensure that a container break-out does not escalate into data extraction from shared volume devices. - network segmentation between containers on the network bridge devices. Exception: When the container serves an Network Function Virtualization role for OSI layer-2, layer-3 or layer-4 function, also regarded as part of data transport network, than this is allowed.
ID	KSP-RE-270
Version	1.0
Date	December 11, 2017
Rationale	System hardening

Requirement	**CIS benchmarks**
Description	Network and server equipment, for which Center for Internet Security (CIS) benchmarks are available, must be hardened as described in these benchmarks, including default configuration values, default account and password blocking. In case of a conflict between the CIS benchmark results and the KSP, the KSP is leading.
Supplement	The CIS Benchmarks are available free of charge in PDF format to anyone via: https://benchmarks.cisecurity.org/downloads/multiform/index.cfm As part of KPN's CIS SecureSuite® Membership, all colleagues can register for an account (using their corporate e-mail address) and get access to CIS-CAT Pro configuration assessment tool, remediation content and full-format CIS Benchmarks at: https://workbench.cisecurity.org/
ID	KSP-RE-260
Version	1.1
Date	May 3, 2019
Rationale	System hardening

Requirement	**Container image layer controle**
Description	Containers must be assembled and build from image layers containing supported software, which can be commercially supported or community supported. All image layers must be kept up to date.
ID	KSP-RE-271
Version	1.0
Date	December 11, 2017
Rationale	System hardening

Requirement	**No CIS benchmarks available**
Description	Network or server equipment, for which Center for Internet Security (CIS) benchmarks are not available (such as applications), must be configured according to the security guidelines from the supplier of the equipment, or if available, application specific guidelines developed by KPN.
ID	KSP-RE-261
Version	1.0
Date	December 11, 2017
Rationale	System hardening

Requirement	**Customer account database separation**
Description	For different (business market) customers, account databases (for example Active Directory or LDAP Directory systems) must at least be logically separated from other customers.
Supplement	Choice of way of separation (logical, physical, combo) and possibly additional detection measures must be determined on a case by case basis, based on contracts with customers and risk analysis.
Related info	KSP-GL-508 - Security Architecture Guidelines
ID	KSP-RE-272
Version	1.2
Date	November 1, 2019
Rationale	System hardening

Requirement	**CIS benchmark scenario choice**
Description	When the CIS benchmarks provide multiple scenarios, the most strict scenario should be followed. Level 1 is a minimum requirement: This means that every deviation on the CIS baseline must be accepted by CISO. Level 2 recommendations: must be configured in (highly) secure environments.Level 2 is mandatory for all services marked as vital.
ID	KSP-RE-262
Version	1.1
Date	April 4, 2018
Rationale	System hardening

Requirement	**System log-on with an administrator or root account is prohibited**
Description	Users with administrator rights must not be able to log on to a system directly to the root, administrator or domain administrator account. The users must log on to the system with their personal and unpriviledged account and elevate their effective rights after initial entry on the system. In effect this means that all entry possible protocols to directly log on to a system, like SSH, RDP, SMB, etc, must be hardened to disallow network log on to these privileged system accounts and allow elevation of effective rights when the user is explicitly privileged to do so on the target system. This must be enforced by configuration deployment, e.g. ansible, puppet or group policies.
ID	KSP-RE-273
Version	1.1
Date	November 2, 2018
Rationale	System hardening

Requirement	**Single use**
Description	Systems must be setup and configured to support one service type or application type (such as web services or database). In a virtualized environment, every Virtual Machine counts as one system.
ID	KSP-RE-263
Version	1.0
Date	December 11, 2017
Rationale	System hardening

Requirement	**Restricted Domain Administrator log on**
Description	Accounts with Domain Administrator privileges must never be used on normal workstations.
ID	KSP-RE-274
Version	1.1
Date	November 2, 2018
Rationale	System hardening

Requirement	**Windows Domain Trusts relationships**
Description	Windows Domains must only be trusted in a one-way non-transitive connection between each other, with a trust relationship exclusively towards KPNNL.LOCAL, i.e. trust KPNNL.LOCAL. Bi-directional trusts, transitive and non-transitive are not allowed.
ID	KSP-RE-275
Version	1.2
Date	November 2, 2018
Rationale	System hardening

Requirement	**Host based protection**
Description	Systems directly connected to the Internet must be equipped with host based protection mechanisms, such as ACLs, firewalls, IDS's.
Supplement	Systems directly connected to the internet (i.e. black zone for zoning) are missing a layer of external protection that therefore must be implemented on the system itself.
ID	KSP-RE-265
Version	1.1
Date	August 9, 2019
Rationale	System hardening

Requirement	Stripping
Description	All systems and applications must be stripped of non-essential functionality. If removal is not possible then the non-essential functions must be disabled.
ID	KSP-RE-266
Version	1.0
Date	December 11, 2017
Rationale	System hardening

Requirement	**Mitigation of non-hardened residual risk**
Description	When certain aspects of a system can’t be hardened, the requirements in the related documents must be consulted to see how to handle mitigation, if possible based on the CVSS score of a non-hardened topic.
ID	KSP-RE-267
Version	1.0
Date	December 11, 2017
Rationale	System hardening

Requirement	**System hardening**
Description	Systems must be subjected to a hardening process conform KSP-RA-259 System hardening to minimize risk of an attack.
Supplement	Not necessary features must be closed and protection mechanisms must be used to make the attack surface as little as possible. Close unnecessary features and ports of operating systems.
ID	KSP-RE-268
Version	1.0
Date	December 11, 2017
Rationale	System hardening
Rationale	Vulnerability scanning- and management
Rationale	Separating environments

Requirement	**End user device hardening**
Description	End user devices must be hardened with respect to user privileges, patching and updates, necessary functionality adequate firewall and up-to-date antivirus/ malware controls.
Supplement	Access to the local configuration of the KPN Endpoint must be managed in order to preserve the standardization, integrity and security level of the KPN Endpoint. All KPN Endpoints must receive updates for antivirus/malware detection on a regular basis.
ID	KSP-RE-269
Version	1.0
Date	December 11, 2017
Rationale	System hardening
Rationale	Vulnerability scanning- and management
Rationale	Separating environments

Requirement	**Elevated rights**
Description	Applications or programs may exclusively be started with elevated rights when there is a technical need, but must not execute tasks with elevated rights.
Supplement	For example: a web-service or database. It is allowed to execute tasks with elevated rights when these tasks service a system administrative role. For example: Puppet, Ansible or GPO-deployment.
ID	KSP-RE-694
Version	1.2
Date	November 2, 2018
Rationale	System hardening

Requirement	**Wireless connectivity to control and maintain objects**
Description	It is forbidden to control or maintain any object used for services, service components, or applications using any type of wireless connectivity past the stepping stone (i.e. wireless connectivity is allowed upto the stepping stone, after the stepping stone the connection must be wired). Examples of forbidden wireless connectivity is: Wi-Fi Bluetooth Infra-red Mobile network Other radio-based solutions using any type of antenna NFC-based solution with a maximum usage of 20 centimeters or less from (virtual) card to reader is allowed.
Supplement	Radio based control and maintenance is susceptible to security, safety and continuity risks due to electro-magnetic disturbances and unable to control the object, man-in-the-middle attacks, circumvention of physical (access) controls and barriers due to radio leakage through walls.
ID	KSP-RE-754
Version	1.1
Date	August 9, 2019
Rationale	WLAN security
Rationale	Separating environments

Requirement	**Maintenance of services**
Description	Technical management must be performed through a stepping-stone or a dedicated maintenance interface supplied by the cloud provider. Functional maintence can be performed both through the technical management interface as per production interface. For functional maintenance, segregation of duties must be applied between normal user accounts and administative accounts.
Supplement	There is no separate interface, nor a blue zone, in various cloud solutions. Functional and technical management tasks can be located through the front-end interfaces.
ID	KSP-RE-776
Version	1.0
Date	August 9, 2019
Rationale	Remote access
Rationale	Public Cloud
Rationale	SaaS provider

Requirement	**Autorun on usb interfaces**
Description	Autorun should be disabled for usb interfaces (including U3 drives).
Supplement	Autorun on usb/flash devices is an often used means to spread malware or gain access to devices.
ID	KSP-RE-767
Version	1.0
Date	August 9, 2019
Rationale	System hardening

Requirement	**TV STB Spoofing**
Description	It must not be possible for the customer to change the MAC settings of a TV Set Top Box from the user interface.
Supplement	By changing MAC setting a customer might be able to simulate the device of another user and gain access to data or content they should not be able to access.
ID	KSP-RE-768
Version	1.0
Date	August 9, 2019
Rationale	System hardening

Requirement	**Software and configuration updates for CPE**
Description	To protect the customer software, firmware and configuration changes may only be accepted from authenticated sources/manufacturers. Example control: Firmware/Software and configuration updates need to be signed with a digital certificate, matching the root certificate within the CPE. This mechanism is called ‘Code Signing’ and the CPE will check the certificate prior to installing the firmware/software.
Supplement	Prevent unauthorized changes to a CPE by authenticating the source before allowing the change. An alternative control can be loading firmware/software and configuration using a secured channel, such as authenticated TR-069 or authenticated use of file transfer over https.
ID	KSP-RE-769
Version	1.0
Date	August 9, 2019
Rationale	System hardening