

Overview of selected KPN Security Policies

Creation date: Wednesday, December 4, 2019 12:52:02 PM

Selected by: Ruud Leurs

| | |
|--------------------|---|
| Requirement | Defining and documenting authorizations |
| Description | Authorizations within a system must be defined and documented. |
| Supplement | <p>To allow consistent assignment of authorizations in the system and to enable periodic review the correctness.</p> <p>Authorizations can be documented in Function Authorization Matrix (FAM), which can vary from a 1 to 1 matrix (there is only 1 function for all users) to matrix with many functions in different segments to many system resources.</p> |
| ID | KSP-RE-372 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Central identity and access management |

| | |
|--------------------|--|
| Requirement | Perform an (information) security risk assessment |
| Description | <p>Prior to purchasing or using cloud services an (information) security risk assessment must be performed, which takes into account:</p> <p>the type, classification and importance of information that may be handled in the cloud (e.g., commercial information, financial information, intellectual property (IP), legal, regulatory and privileged information (LRP), logistical information, management information or personally identifiable information (PII)).</p> |
| Supplement | This is part of the cloud governance process. |
| ID | KSP-RE-98 |
| Version | 1.1 |
| Date | May 3, 2019 |
| Rationale | Information classification |
| Rationale | Cloud Computing |
| Rationale | Public Cloud |
| Rationale | SaaS provider |
| Rationale | Private Cloud |

| Requirement | Portal Authority |
|---------------------|---|
| Description | <p>The following KPN products and services must be tested by the KPN Portal Authority:</p> <p>new or upgraded products and services that are accessible via the internet;</p> <p>products and services where we connect one of our brand names to;</p> <p>security products and services used within KPN;</p> <p>high profile / impact applications or devices used within KPN.</p> <p>None of these products and/or services may go live without the permission of the Portal Authority.</p> |
| Related info | Portal Authority info page on TEAMKPN |
| ID | KSP-RE-12 |
| Version | 1.2 |
| Date | August 9, 2019 |
| Rationale | Security testing to innovation and development |
| Rationale | Web-based and other application software |

| | |
|--------------------|---|
| Requirement | Use of biometrics for authentication on mobile devices (phones, tablets and laptops) |
| Description | Biometrics are not allowed as part of a multi factor authentication process, but only as a means to unlock credentials stored in a hardware secure vault solution. E.g. Apple TouchID, Apple FaceID, and fingerprint sensors on Samsung S5 devices or later are acceptable solutions as they all use a secure hardware vault solution to store the fingerprint details. Also Windows Hello is allowed as a biometric solution, assuming the credentials are protected on the device using a TPM 2.0 chip. |
| Supplement | Biometrics on mobile devices and/or PCs have, at this time, vulnerabilities allowing them to be spoofed by a malicious attacker. Therefore they may never be used as a means of authenticating a user. See KSP-RE-247 for the requirement and list of technically accepted authentication solutions. |
| ID | KSP-RE-242 |
| Version | 1.1 |
| Date | August 16, 2018 |
| Rationale | Authentication |

| Requirement | Authentication methods |
|---------------------|---|
| Description | Systems must authenticate users based on username and password and, if required, a second factor. The authentication method must comply to the level defined in KSP-GL-713 and the technical and procedural requirements set in KSP-GL-712. The authentication method must be traceable to a natural person unique user and shall not be copied or expire within a short period of time frame (e.g. 5 minutes). |
| Supplement | Some applications and/or systems have a higher value for KPN and therefore have stricter security requirements. To make sure that the authentication procedure only lets in the correct users certain technical and procedural measures must be in place to support these security requirements. Technically strong authentication methods must be accompanied by an equally strong identity verification procedure in the enrolment of an account. |
| Related info | |
| ID | KSP-RE-247 |
| Version | 2.0 |
| Date | August 16, 2018 |
| Rationale | Authentication |
| Rationale | BYOD (Bring Your Own Device) |
| Rationale | Cryptography generic |

| | |
|--------------------|--|
| Requirement | User authentication |
| Description | End-users must logon to the KPN End User Device using their personal user account and credentials, whereby two-factor authentication is necessary for remote access and signed/encrypted mail. |
| Supplement | If a KPN user access a KPN device, including Bring-Your-Own devices, then he/she must authenticate with his/her KPN credentials. |
| ID | KSP-RE-249 |
| Version | 1.1 |
| Date | August 16, 2018 |
| Rationale | Authentication |

| | |
|--------------------|--|
| Requirement | Inventory of authorization decisions |
| Description | Each application, system and network element must have an up to date administration registering the current granted accounts and authorizations and who authorised these (manager and additional authorisers) and at what time. |
| Supplement | <p>For all existing accounts and authorizations must be traceable who authorised whom and at what time. Therefore an account/authorization request must be registered including who authorised whom and when.</p> <p>Excel list with agree of managers and second authorizers.</p> |
| ID | KSP-RE-373 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Central identity and access management |

| | |
|--------------------|--|
| Requirement | Integrity and reliability of logging |
| Description | Logging must be carried out in such way, that the log data can be used as evidence in possible court cases. This means that the integrity and availability of this data must be guaranteed and manipulation of log data is not possible. |
| Supplement | The implementation of this requirement is assigned to the administrator of the central log platform. |
| ID | KSP-RE-496 |
| Version | 1.1 |
| Date | June 18, 2018 |
| Rationale | Logging |
| Rationale | Law and regulation |

| | |
|--------------------|--|
| Requirement | Acting upon log events |
| Description | Log data must be analyzed structurally, at least daily. If suspicious events are detected from log file analysis, this should be treated as a security incident. |
| ID | KSP-RE-500 |
| Version | 1.1 |
| Date | November 2, 2018 |
| Rationale | Logging |

| | |
|--------------------|--|
| Requirement | Retention period central logs |
| Description | <p>The period for storing centralized logs must be set to 180 days. Unless the type of logs does not allow it. In this case, the owner determines the retention time.</p> <p>When the log data is needed after 180 days, the logs must be aggregated in such way that they can no longer be traced back to individuals.</p> |
| ID | KSP-RE-503 |
| Version | 2.0 |
| Date | June 18, 2018 |
| Rationale | Logging |

| | |
|--------------------|--|
| Requirement | Vulnerability scanning |
| Description | All KPN assets connected to a network, must be scanned for vulnerabilities on a minimum monthly basis. All interfaces, including the logical and external interfaces, must be scanned. The asset owner of the system on which the vulnerabilities have been found must take measures in response to the findings. |
| Supplement | <p>Customers' assets that are part of the KPN network are not in scope for vulnerability scanning.</p> <p>Vulnerability management on KPN assets with an interface in a black zone, not being Internet or KOEN, may deviate from this rule if other, by CISO approved ways, regular management of vulnerabilities are met.</p> |
| ID | KSP-RE-253 |
| Version | 1.1 |
| Date | November 2, 2018 |
| Rationale | Vulnerability scanning- and management |

| | |
|--------------------|---|
| Requirement | Centrally managed vulnerability scanning |
| Description | Vulnerability scanning must be managed centrally and managed for the entire KPN organization. |
| ID | KSP-RE-254 |
| Version | 1.1 |
| Date | November 2, 2018 |
| Rationale | Vulnerability scanning- and management |

| Requirement | Vulnerability mitigation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------------------|--|------------------------------|----------------|--------------------|------------------|------------------|--------------------|------------------|--------------------|--|--|-----------|--------|--|--|--|--|--|--|------|-------|----------|------------|----------|------|--|--------|--|-----|----------|--------|----------|------------------|--|----------|------|--------|--|-----|------|---------|----------|--------|--|--|----------|------|--------|-----|--------|---------|----------|-------|--|--|--|----------|------|---------|-----|---------|
| Description | <p>Identified vulnerabilities (whether found based on the monthly vulnerability scanning, or found through other means) must be fixed according to the following timelines:</p> <table><tr><th colspan="2">Priority and solution time →</th><th>ONE immediately</th><th>TWO 2 weeks</th><th>THREE 1 month</th><th>FOUR 2 months</th><th>FIVE 6 months</th><th>SIX best effort</th><th></th><th></th></tr><tr><th>Scanner ↓</th><th>Zone ↓</th><th></th><th></th><th></th><th></th><th></th><th></th><th>CVSS</th><th>Score</th></tr><tr><td>external</td><td>black, red</td><td>critical</td><td>high</td><td></td><td>medium</td><td></td><td>low</td><td>critical</td><td>9 - 10</td></tr><tr><td>internal</td><td>black, red, blue</td><td></td><td>critical</td><td>high</td><td>medium</td><td></td><td>low</td><td>high</td><td>7 - 8.9</td></tr><tr><td>internal</td><td>orange</td><td></td><td></td><td>critical</td><td>high</td><td>medium</td><td>low</td><td>medium</td><td>4 - 6.9</td></tr><tr><td>internal</td><td>green</td><td></td><td></td><td></td><td>critical</td><td>high</td><td>med-low</td><td>low</td><td>0 - 3.9</td></tr></table> <p>If a vulnerability cannot be fixed, mitigating measures must be implemented according to the timeframe.</p> | Priority and solution time → | | ONE immediately | TWO 2 weeks | THREE 1 month | FOUR 2 months | FIVE 6 months | SIX best effort | | | Scanner ↓ | Zone ↓ | | | | | | | CVSS | Score | external | black, red | critical | high | | medium | | low | critical | 9 - 10 | internal | black, red, blue | | critical | high | medium | | low | high | 7 - 8.9 | internal | orange | | | critical | high | medium | low | medium | 4 - 6.9 | internal | green | | | | critical | high | med-low | low | 0 - 3.9 |
| Priority and solution time → | | ONE immediately | TWO 2 weeks | THREE 1 month | FOUR 2 months | FIVE 6 months | SIX best effort | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Scanner ↓ | Zone ↓ | | | | | | | CVSS | Score | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| external | black, red | critical | high | | medium | | low | critical | 9 - 10 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| internal | black, red, blue | | critical | high | medium | | low | high | 7 - 8.9 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| internal | orange | | | critical | high | medium | low | medium | 4 - 6.9 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| internal | green | | | | critical | high | med-low | low | 0 - 3.9 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Supplement | <p>Categories of vulnerabilities</p> <p># External: Internet facing</p> <p>Vulnerabilities detected from an external scanner / the Internet.</p> <p># Internal: not-Internet facing</p> <p>Vulnerabilities detected on the inside.</p> <p>Scoring on</p> <p># CVSS version 3: critical, high, medium and low*</p> <p># Zones: black, red, orange, green and blue</p> <p>* Common Vulnerability Scoring System (CVSS) Score. Several vendors have their own definition of Low/Medium/High/Critical. To not be tied to a specific product or vendor, the priorities are based on CVSS v3 Base scores.</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ID | KSP-RE-255 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Version | 2.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Date | February 20, 2019 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rationale | Vulnerability scanning- and management | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | |
|--------------------|---|
| Requirement | Updates |
| Description | Security updates must be installed per the timelines set in KSP-RE-255 (Vulnerability mitigation) on all KPN assets. This must be verified regularly. Deviations must be resolved as quickly as possible. |
| ID | KSP-RE-256 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Vulnerability scanning- and management |

| | |
|--------------------|--|
| Requirement | Vulnerability management process |
| Description | A vulnerability management process must be implemented and followed. |
| ID | KSP-RE-257 |
| Version | 1.2 |
| Date | May 3, 2019 |
| Rationale | Vulnerability scanning- and management |

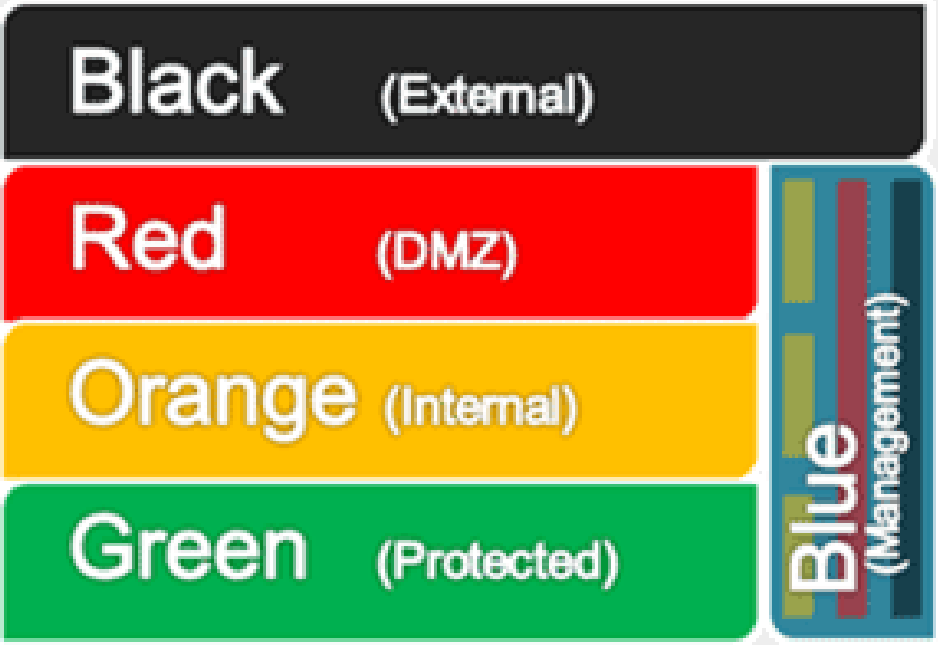
| | |
|--------------------|---|
| Requirement | Vulnerability Management |
| Description | Every system is to be scanned for vulnerabilities on a regular basis. The resulting findings need to be resolved within a pre-defined timeframe depending on the severity. |
| Supplement | <p>Vulnerabilities can arise over time and must be solved timely to keep the system sufficient safe for attacks.</p> <p>i.e. Schedule of vulnerability tests for systems</p> <p>Isolated systems (without network link and no mobile storage applicable) have no need for vulnerability management.</p> |
| ID | KSP-RE-258 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Vulnerability scanning- and management |

| | |
|--------------------|---|
| Requirement | Logical network separation and services |
| Description | <p>Services must be separated from each other by usage of logical network separation. If a service spans multiple zones, it must have a separate logical network for every zone.</p> <p>If a service is composed out of multiple (smaller) sub-services, the services must be separated from each other.</p> <p>For infrastructures identified as vital infrastructure the network separation must not be performed nor dependent upon a hypervisor or container.</p> <p>Example technology:</p> <p>VLAN's, Q-in-Q, VXLAN, Private VLAN, VRF, Oracle Solaris Zones.</p> |
| ID | KSP-RE-280 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Separating environments |

| | |
|--------------------|--|
| Requirement | Communication between logical networks |
| Description | <p>When a system has multiple logical network connections in a zone, routing between them must be disabled by default.</p> <p>Where routing between logical networks is necessary, traffic that passes the boundary between these networks must be filtered.</p> |
| ID | KSP-RE-281 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Separating environments |

| | |
|--------------------|--|
| Requirement | Communication between services |
| Description | <p>Communication between services must be done through a common production zone (i.e. red, orange or green).</p> <p>An alternative is possible when communicating to central services, e.g. Microsoft Active Directory for authentication and account synchronisation. The communication must be configured with a stateful firewall in such a way that the establishment of the connection's initiative is exclusively from the relying service to the central service.</p> |
| ID | KSP-RE-282 |
| Version | 2.0 |
| Date | February 1, 2019 |
| Rationale | Separating environments |
| Rationale | Documenting network infrastructure |
| Rationale | Encrypting network traffic |
| Rationale | Designing to availability level |

| Requirement | Requirements for non-production platforms |
|--------------------|---|
| Description | <p>Platforms for development or testing, and platforms for acceptance of operational software must be separated in sufficient degree of each other and of the live environment. The acceptance environment need to resemble the live platform in architecture and setup. Tests must be conducted on a test platform.</p> <p>The use of sensitive information (e.g. privacy, business obligations) in a development and test environment is explicitly forbidden. In an acceptance environment that meets the KSP, and that has the same security level as the production environment, use is allowed.</p> |
| Supplement | <p>Testing the change in the production environment poses extra risks because of possible unexpected behaviour due to the change.</p> <p>The use of real customer and user data exposes this data to loss, disclosure and access to this by not authorised people.</p> <p>When test data will not reveal enough assurance (e.g. compare test results with operational results) so real data must be used; then all security measures for production data must be taken for the test platform and permission from the Operational Security Manager or, depending on the datatype, Senior Security Officer or Privacy officer must be obtained prior to the start of the test activities.</p> |
| ID | KSP-RE-286 |
| Version | 1.5 |
| Date | December 7, 2018 |
| Rationale | Separating environments |

| Requirement | Network segmentation and security zoning |
|--------------------|--|
| Description | <p>Segments must be defined and implemented for a network environment to support a layered security model.</p> <p>This can be achieved by building services in accordance to a security zoning model. The following is a high-level description of the KPN standard zoning model:</p>  <p>A typical service would have the systems users (who are in the Black zone) need to interact with in the Red zone, systems that are purely for service internal use in the Orange zone and servers containing confidential data in the Green zone. All systems also need a connection into the Blue zone in order to be managed. Communication between services is prescribed in KSP-RE-282.</p> <p>The internal network KOEN is classified as a black zone.</p> <p>Customer IaaS and PaaS environments must be segmented.</p> |
| Supplement | <p>Just as in physical security, not everything happens in one room. Network segments should have a specific purpose and should be separated from other segments with their specific purpose. Segmentation must be done on function and classification of network data.</p> <p>Segmentation can be applied using a variety of technologies which includes and is not limited to MPLS tags, VLAN, VXLANs, virtual networks and other overlay technology.</p> <p>Direct communication to generic services, e.g. Active Directory, is conditional to KSP-RE-282.</p> <p>A webserver that is used for serving webpages to internet should not be in the same segment as the backup system for this server.</p> |

| | |
|------------------|----------------------------|
| ID | KSP-RE-287 |
| Version | 1.2 |
| Date | November 1, 2019 |
| Rationale | Separating environments |
| Rationale | Encrypting network traffic |
| Rationale | WLAN security |

| | |
|--------------------|--|
| Requirement | Network filtering |
| Description | Between network segments a network filter must be in place through which only necessary traffic can pass. |
| Supplement | <p>Network segments are defined because of their different uses, security wise and functionality wise. To keep these separated, filtering of networking traffic is necessary.</p> <p>A webserver may need a database server backend to be able to serve content to clients. This communication must be limited to only the necessary database communication to prevent misuse. This communication is registered in a communication matrix.</p> |
| ID | KSP-RE-288 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | Separating environments |

| | |
|---------------------|--|
| Requirement | Applications sharing a platform |
| Description | Applications must not share the same platform when they do not have the same data-classification. When more than one application is hosted on a platform, the highest security demanding application will determine the minimal security requirements. |
| Related info | |
| ID | KSP-RE-289 |
| Version | 1.1 |
| Date | February 1, 2019 |
| Rationale | Separating environments |

| | |
|--------------------|---|
| Requirement | Filtering traffic |
| Description | <p>Traffic that passes a zone boundary inbound or outbound must be filtered with firewalls. Any traffic that isn't explicitly allowed and registered in a communication matrix must be denied and logged.</p> <p>Cloud resources must be segmented and zoned using stateful firewalls.</p> <p>Changes to the traffic filters must follow change management rules for the asset and the change to be registered.</p> |
| ID | KSP-RE-279 |
| Version | 1.2 |
| Date | November 1, 2019 |
| Rationale | Separating environments |

| | |
|--------------------|--|
| Requirement | Container segmentation and zoning |
| Description | <p>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:</p> <ul style="list-style-type: none"> - 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. <p>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.</p> |
| ID | KSP-RE-270 |
| Version | 1.0 |
| Date | December 11, 2017 |
| Rationale | System hardening |

| | |
|--------------------|--|
| Requirement | CIS benchmarks |
| Description | <p>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.</p> <p>In case of a conflict between the CIS benchmark results and the KSP, the KSP is leading.</p> |
| Supplement | <p>The CIS Benchmarks are available free of charge in PDF format to anyone via: https://benchmarks.cisecurity.org/downloads/multiform/index.cfm</p> <p>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/</p> |
| ID | KSP-RE-260 |
| Version | 1.1 |
| Date | May 3, 2019 |
| 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 | 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 unprivileged 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 | 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 | Encryption of data at rest |
| Description | Encryption of all data at rest is obligatory in cloud resources. For data in KPN data centers it is obligatory to encrypt information classified as Secret. Confidential data is advised to be stored in encrypted form. |
| Supplement | <p>For cloud resources the following solutions are accepted:</p> <p>AWS KMS</p> <p>AWS CloudHSM</p> <p>Azure Key Vault</p> <p>Hashicorp KeyVault</p> <p>Bring-Your-Own-Key methods are also allowed, assuming they key custodianship with backup policy for the key material is on-par with the solution. It is recommended to ask advice at CISO before using BYOK for business continuity reasons.</p> <p>For other solutions advice is required.</p> |
| ID | KSP-RE-318 |
| Version | 2.0 |
| Date | May 3, 2019 |
| Rationale | Web-based and other application software |
| Rationale | Information classification |
| Rationale | Cryptography generic |

| | |
|--------------------|---|
| 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 | Logging of security events |
| Description | Networks and systems need to log security events. KPN-CERT may require additional logging due to security incident response and / or investigations. |
| Supplement | We distinguish the following types of log sources: application, daemon, OS, network element and hardware. Guideline KSP-GL-508 refers to detailed instruction regarding the type of security events that should be logged. |
| ID | KSP-RE-699 |
| Version | 1.1 |
| Date | November 2, 2018 |

| | |
|--------------------|--|
| Requirement | Secure connectivity between a cloud and KPN data centers |
| Description | <p>Backhaul connectivity from the cloud services to KPN data centers must use a AWS Direct Connect or Microsoft Express Route.</p> <p>An alternative is by using a VPN, e.g. an IPSec tunnel.</p> <p>Traffic to and from SaaS solution is excluded from this rule. For example, SaaS solutions from external suppliers and KPN's use of Office365.</p> |
| ID | KSP-RE-740 |
| Version | 2.0 |
| Date | May 3, 2019 |

| | |
|--------------------|---|
| Requirement | Presence of an exit strategy on cloud services |
| Description | A data and service exit strategy must be in place before operating with a Cloud Service Provider (CSP). |
| ID | KSP-RE-742 |
| Version | 1.0 |
| Date | November 2, 2018 |

| | |
|--------------------|---|
| Requirement | Avoidance of (temporary) cloud service destruction |
| Description | Financial control must be in place to avoid the (temporary) destruction of a cloud service, due to not paying in time. Reinstating the service as-is must not be assumed. |
| ID | KSP-RE-741 |
| Version | 1.0 |
| Date | November 2, 2018 |

| | |
|--------------------|--|
| Requirement | Use of a credential vault solution |
| Description | The Cloud Service Provider (CSP) must use a credential vault solution that is controlled by KPN. |
| Supplement | Some options are: Azure Key Vault Hashicorp Vault |
| ID | KSP-RE-743 |
| Version | 1.1 |
| Date | May 3, 2019 |

| | |
|--------------------|--|
| Requirement | Cloud controls |
| Description | The responsible DevOps teams have the obligation to set up the cloud service in the environment which has been set up according to specific agreements with KPN. This environment must feature technical controls aligning with the KSP to ensure the tools and infrastructure in KPN's cloud tenants are secured and continuously monitored. Before moving to production all controls must be proven to be compliant. These cloud controls are configured and maintained by the Cloud Platform Teams, not by the DevOps teams to ensure segregation of duty. The DevOps teams have the obligation to act upon the alarms triggered by the cloud controls. |
| ID | KSP-RE-765 |
| Version | 1.1 |
| Date | November 1, 2019 |

| | |
|--------------------|---|
| Requirement | Cloud resources |
| Description | Cloud resources of all technical types must show a positive result from the technical compliance report in the cloud before letting the resources work as production resources. |
| Supplement | <p>Elements that have to be in technical compliant are, but not limited to:</p> <p>Encryption of data at rest;</p> <p>Encryption of data in transit;</p> <p>Use of stateful firewalls for segmentation and zoning in te cloud;</p> <p>IAM to the assets, with appropriate account structures, roles, and privilege separation;</p> <p>Asset management;</p> <p>BCM process;</p> <p>System hardening;</p> <p>Security information, event management and logging.</p> |
| ID | KSP-RE-762 |
| Version | 1.0 |
| Date | May 3, 2019 |

| | |
|--------------------|--|
| Requirement | Vulnerability management in the cloud |
| Description | <p>Vulnerability management in the cloud is mandatory on IaaS and PaaS resource types.</p> <p>Resources which are build and maintained by the cloud provider are excluded.</p> <p>SaaS solutions from suppliers are excluded, unless specific agreements have been made.</p> |
| ID | KSP-RE-763 |
| Version | 1.0 |
| Date | May 3, 2019 |

| | |
|--------------------|---|
| Requirement | Special high privileged accounts |
| Description | <p>Privileges assigned to accounts or groups which have the power to damage the infrastructure directly must be protected with:</p> <p>4-eyes principle: at least two people must be present during activities and this must be auditable.</p> <p>The workstations from which the activities are conducted must be able to be logged via the central log management facilities.</p> <p>The activities must be conducted from KPN building and the internal network, i.e. KOEN_Wlan.</p> |
| Supplement | <p>For Amazon AWS additional attention is required to the Master Biller Account and subsequent high privileged accounts.</p> <p>For Microsoft Azure additional attention is required to all users in the Global Administrator and Security Administrator groups.</p> <p>As the account privileges and account management is founded in KPN's Microsoft Active Directory and IAM Portal systems, special attention must be given to all users part of the Domain Administrators group and all systems with similar privileges.</p> |
| ID | KSP-RE-761 |
| Version | 1.1 |
| Date | August 9, 2019 |