Friday, April 20, 2018 10:22:47 AM

Ruud Leurs

Requirement	**Sharing of infrastructure**
Description	Multiple applications may store their data on a shared database, but must fulfill the following requirements: - The security risk profile of all applications must be the same. i.e. for nationally defined vital infrastructure services the database must not be shared with non-vital infrastructure services. - The applications shared on the platform must have similar uptime and ata loss requirements.
ID	KSP-RE-440
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Access to database**
Description	One application may connect to multiple databases, but must fulfill the following requirements: - The application must ask for written permission from the respective administrators, the owner of the connected application(s), and the owner(s) of the data for all connected databases. This written permission must explicitly allow the interconnection between all other databases and be given for every (new) connection; - the application acting as a data hub must adhere to the combined security requirements fo all connected databases; - the application one has the rights to acces and is only able to manipulate the data as required for its correct functioning.
ID	KSP-RE-441
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Screening of database administrators**
Description	Database administrators must be screened according to the content and value of the database and the data within.
ID	KSP-RE-442
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Database Backup security**
Description	The backup of data must be secure with the same or stricter security means as the production environment.
ID	KSP-RE-443
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Security standard for databases**
Description	The storage of data in a database must be done securely to prevent unauthorized access and, indirectly, fines by third parties.
ID	KSP-RE-444
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Access to data on disk**
Description	The data on disk must not be accessible to people that do not have access. If a person has rights then this must be limited to whatever is required for them to fulfill their role.
ID	KSP-RE-445
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Database hardening**
Description	Datastorage solutions, e.g. databases, file shares, sharepoint, NAS, SAN, etc, must be hardened according to best practises from the hardening guidelines. The KSP is leading in case of a conflict.
ID	KSP-RE-446
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Database auditing**
Description	Access to the data stored in a database must be auditable via sufficient logging.
ID	KSP-RE-447
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Data transport encryption**
Description	When transporting data, physically or digitally, the use of encryption is mandatory.
ID	KSP-RE-448
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Zoning and segmentation for databases**
Description	Databases must be hosted on a platform which adheres to the network segmentation and zoning requirements. Databases that contain credentials, Personally identifiable information or information classified as internal or secret must reside in a green zone.
ID	KSP-RE-438
Version	1.1
Date	April 4, 2018
Rationale	Database protection

Requirement	**Disk encryption of databases**
Description	Disk encryption is not required for a database if all rules are verified to be in-place, auditable, and the data is stored in a KPN owned datacenter.
ID	KSP-RE-449
Version	1.0
Date	December 11, 2017
Rationale	Database protection

Requirement	**Network segmentation and zoning for databases**
Description	Applications that do not have access rights to a database must not be able to reach the database over a network. If an unauthorised attempt is made to access the database it should be logged and immediately sent to a central logging entity.
ID	KSP-RE-439
Version	1.0
Date	December 11, 2017
Rationale	Database protection