Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 8:25:07 PM

Selected by: Ruud Leurs

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	**Centralized logging**
Description	All logs must be forwarded to the central logmanagement platform of KPN. Within five minutes after the occurrence of the event log data must reside on the central logmanagement platform.
Supplement	KPN collects the logs of security events in KPN's networks and systems in a dedicated **central** log management platform. Guideline GL-508 refers to detailed instruction on setting up a log aggregator, an initial log collector (ILC) and realizing connectivity to the central platform.
ID	KSP-RE-499
Version	1.1
Date	June 18, 2018
Rationale	Logging

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	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. 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.
ID	KSP-RE-503
Version	2.0
Date	June 18, 2018
Rationale	Logging

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