Overview of selected
KPN Security Policies

Creation date: Wednesday, November 7, 2018 8:12:07 PM

Selected by: Ruud Leurs

Requirement	**Scan of external files**
Description	All data, software, email and other files being downloaded from external sources (including removable media) must be checked automatically with authorized anti-virus software for malicious software and email filtering, even in the case of an authorized source.
ID	KSP-RE-291
Version	1.1
Date	November 2, 2018
Rationale	Protection against malware

Requirement	**Centralized protection solution**
Description	The malware protection measures used by device management parties must be centralized, automated and working without intervention (user- transparent); deactivation or bypassing of the protection against malicious software by the user must be prohibited: • Ability to disable the antivirus services; • Ability to disable or cancel a scheduled scan; • Ability to disable real time scanning; • Ability to modify scan policies. Attempts must be logged and sent to a central logging entity
ID	KSP-RE-292
Version	1.0
Date	December 11, 2017
Rationale	Protection against malware

Requirement	**Protection of Mobile Computers and Teleworking Systems**
Description	The malware protection software must be automatically updated (with new configuration settings, new libraries and new versions of the software) when these devices are connected to the corporate network directly or remotely. Mobile computers and teleworking systems that have not connected and been updated for 3 months or longer must first be updated and scanned before a new connection is allowed.
Supplement	Updates can be limited to maintenance windows or be stopped during calm periods.
ID	KSP-RE-293
Version	1.0
Date	December 11, 2017
Rationale	Protection against malware

Requirement	**Anti Virus Software version and library updates**
Description	Anti- Virus software libraries- and version updates must immediately be updated after their release by software vendors.
ID	KSP-RE-294
Version	1.1
Date	November 2, 2018
Rationale	Protection against malware

Requirement	**Full scan**
Description	Periodically all files on all workstations and servers must be scanned for malware. For performance reasons, this may be an iterative scan. Scan cycles must be run as frequent as possible. The interval between two cycles must not be greater than 1 month. For file-shares, dropzones, FTP servers or managed file transfer services the files must be scanned (within the scope of the dropzone) with a scan on-access policy.
ID	KSP-RE-295
Version	1.1
Date	November 2, 2018
Rationale	Protection against malware

Requirement	**Access protection**
Description	The anti-malware solution must, at a minimum, have anti-tamper mechanisms, status/health checks, memory and buffer overflow protection in place. If a health check fails or if deactivation or bypass of these mechanisms is detected this must result in an alarm being logged and sent to the responsible department and KPN SOC.
ID	KSP-RE-296
Version	1.1
Date	November 2, 2018
Rationale	Protection against malware

Requirement	**Automated tools**
Description	Automated tools must be deployed to monitor workstations, severs, and mobile devices . This tool must, at a minimum, support signature based, behavioural, heuristic, and script based checks for both file and network traffic.
ID	KSP-RE-297
Version	1.0
Date	December 11, 2017
Rationale	Protection against malware

Requirement	**Event management**
Description	All malware detection events must be sent to enterprise anti-malware administration tool and event log servers. The alerts must be automatically dispatched to the responsible department and KPN SOC.
ID	KSP-RE-298
Version	1.1
Date	November 2, 2018
Rationale	Protection against malware
Rationale	Logging

Requirement	**Updates of anti-malware engine**
Description	Besides the daily signature updates, also the anti virus software should be kept up-to-date. If the anti-virus software is updated manually, the vendor’s website should be checked periodically for new updates. After applying an update, automated systems should verify that each system has processed its update.
ID	KSP-RE-299
Version	1.1
Date	November 2, 2018
Rationale	Protection against malware

Requirement	**Signature updates**
Description	Signature auto-update features must be deployed. Checks for updates must be done on a daily basis. After applying an update, automated systems must verify that each system has processed its signature update.
ID	KSP-RE-300
Version	1.0
Date	December 11, 2017
Rationale	Protection against malware

Requirement	**Malware protection**
Description	An up-to-date and supplier supported protection against malware must be set up on the elements on the system where possible.
Supplement	Malware may create a backdoor for unauthorized access on a system.
ID	KSP-RE-301
Version	1.0
Date	December 11, 2017
Rationale	Protection against malware

Requirement	**Certification for Endpoint Protection**
Description	The EPP solution supplier must have passed at least three (3) out of four (4) most recent 'MRG-Effitas 360 degree assessment and certification tests' with a level two (2) certification. Possible exception: upon request, an as-of-yet unspecified solution, can be allowed if it passes two (2) consecutive “MRG-Effitas 360 degree assessment and certification tests” with a level two (2) certification. For consistency, the period between those two tests, must be at least three months. Test conditions and final approval must be obtained from KPN CISO before go-live.
Supplement	The MRG-Effitas tests provide an accurate and independent measurement guideline to follow when choosing a supplier for endpoint protection. For reasons of consistency, multiple consecutive test results are taken into account. More information can be found at MRG-Effitas.com.
ID	KSP-RE-302
Version	1.0
Date	December 11, 2017
Rationale	Protection against malware

Requirement	**Sharing information**
Description	Malware detection must be possible without sharing KPN-related data outside of the company. Insignificant data such as Hashes or PE-Files are excluded of this rule but is sharing is not preffered.
ID	KSP-RE-303
Version	1.0
Date	December 11, 2017
Rationale	Protection against malware

Requirement	**Software maintenance**
Description	Only software versions supported by the supplier must be used.
Supplement	Software not supported by the supplier can lead to a continuity problem when changes or updates that are needed on the system are no longer compatible. So security vulnerabilities will not be fixed. Common off the shelve (COTS) software is often sold with maintenance guarantees. For Freeware or other sofware not managed by a supplier an exception must be approved.
ID	KSP-RE-304
Version	1.1
Date	November 2, 2018
Rationale	Protection against malware
Rationale	Exceptions