

KPN Security Policy



KSP – Rule

| | | |
|-------------|----------------------------------|--|
| Title | Malware protection | |
| ID | KSP-FA05-RL05 | |
| Funct. Area | 05 – System and Network security | |
| Date | 2 November 2016 | |
| Version | v2.4 | |
| Status | Approved | |
| Owner | CISO | |

Summary

This document defines the requirements needed to protect against malicious software. This rule document is applicable for each device linked with KPN that is susceptible to malicious software, i.e. that is not isolated from any network. Proven not-susceptible devices are out of scope.

Version history

| Version | Date | Comments |
|---------|-------------------|--|
| v1.0 | 17 September 2013 | Approved in SSM |
| v1.1 | 9 October 2013 | Updated based on consistency check |
| v2.0 | 4 April 2014 | Updated based on feedback in Q4 2013 and Q1 2014; KPN generic elements of ITS anti-malware policy adopted |
| v2.1 | 1 August 2014 | Q2 policy update (extensive rework but no changes on essentials, some overlapping rules combined into 1, R05 removed as it conflicted with FA06-RL01) |
| v2.2 | 13 November 2015 | Yearly review; only textual changes made. |
| V2.3 | 29 July 2016 | R02: adjusted with a proper scope and choices are bound by the integrity checks from a platform. R08: automatic update removed, the immediate update is not changed (prio update). R09: scan cycle must not exceed 2 months. For dropzones there is an on-access policy. |
| v2.4 | 2 November 2016 | R01: changed disk sharing to file sharing |

Disclaimer

The content of this document is to describe KPN's policy on this specific topic. If and when this document is partly or fully disclosed to parties outside of KPN, it's important to hereby note towards those parties that this contains KPN's intended policy and cannot in any way be read or construed to be an explicit or implied formal guarantee or promise that its content can always be fully executed or complied to.

| | |
|--------------------------|--|
| ID | KSP-FA05-RL05-R01 |
| Title | <u>File sharing</u> |
| Description | The use of the file sharing features on a PC or mobile device is prohibited. This includes the sharing of a (virtual) disk, directory or file via an interface, like the network. |
| Relating document | N/A |

| | |
|--------------------------|---|
| ID | KSP-FA05-RL05-R02 |
| Title | <u>Software from untrusted sources</u> |
| Description | <p>Software originating from sources other than the authorized source for a domain must not be used, installed or copied on KPN systems because such software can contain viruses, worms, Trojan horses, keyloggers, espionage-software, etc.</p> <ul style="list-style-type: none"> • (Mobile) apps must be traceable back to the author • The integrity of the app must be guaranteed by the integrity controls provided by the (mobile) platform. • The user is responsible for checking and rejecting (mobile) apps when they are not originating from the expected company. • Disabling and/or tampering with the integrity controls is forbidden. <p>The Google Play Store, AppStore from Apple, Microsoft Windows Store and Mobile Iron (and others) are solutions which use the platform systems integrity mechanisms best.</p> |
| Relating document | N/A |

| | |
|--------------------------|--|
| ID | KSP-FA05-RL05-R03 |
| Title | <u>Scan of external files</u> |
| 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. |
| Relating document | N/A |

| | |
|--------------------------|--|
| ID | KSP-FA05-RL05-R06 |
| Title | <u>Centralized protection solution</u> |
| Description | <p>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:</p> <ul style="list-style-type: none"> • 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. |
| Relating document | N/A |

| | |
|--------------------------|--|
| ID | KSP-FA05-RL05-R07 |
| Title | <u>Protection of Mobile Computers and Teleworking Systems</u> |
| Description | <p>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.</p> <p>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.</p> |
| Relating document | N/A |

| | |
|----------------------------|--|
| ID | KSP-FA05-RL05-R08 |
| Title | <u>Protection Software version and library updates</u> |
| Description | Protection software (against malicious software) libraries- and version updates must immediately be updated after their release by software vendors. |
| Relating document | N/A |
| Possible exceptions | Updates might be limited to change windows or stopped during freeze periods. |

| | |
|--------------------------|--|
| ID | KSP-FA05-RL05-R09 |
| Title | <u>Full scan</u> |
| Description | <p>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.</p> <p>The interval between two cycles must not be greater than 2 months. 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.</p> |
| Relating document | N/A |

| | |
|--------------------------|---|
| ID | KSP-FA05-RL05-R10 |
| Title | <u>Access protection</u> |
| Description | Besides pattern and heuristic malware scanning, anti-malware software must also support script scanning, buffer overflow protection and anti-tampering functionality (“Access Protection”). |
| Relating document | N/A |

| | |
|--------------------------|---|
| ID | KSP-FA05-RL05-R11 |
| Title | <u>Automated tools</u> |
| Description | Automated tools must be deployed to monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. |
| Relating document | N/A |

| | |
|--------------------------|--|
| ID | KSP-FA05-RL05-R12 |
| Title | <u>Event management</u> |
| 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 correct administration teams by this tooling. |
| Relating document | KSP-FA05-RL06 - Logging and monitoring |

| | |
|--------------------------|--|
| ID | KSP-FA05-RL05-R13 |
| Title | <u>Updates of anti-malware engine</u> |
| Description | Besides the daily signature updates, also the anti-malware engine should be kept up-to-date. If the anti-malware engine 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. |
| Relating document | N/A |

| | |
|--------------------------|---|
| ID | KSP-FA05-RL05-R14 |
| Title | <u>Signature updates</u> |
| 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. |
| Relating document | N/A |