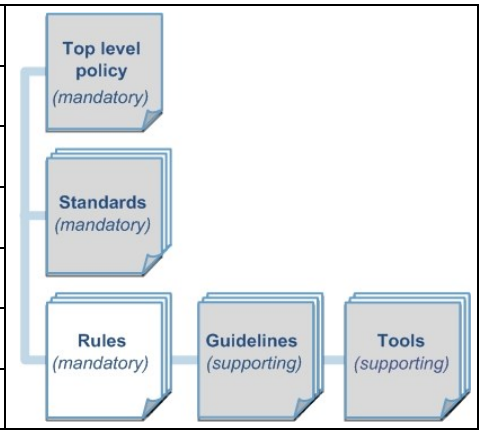
KPN Security Policy

KSP – Rule

Title	**Technical Vulnerability Management**
ID	**KSP-FA05-RL03**
Funct. Area	05 - System and Network Security
Date	3 February 2017
Version	v2.6
Status	Approved
Owner	CISO



Summary

Purpose of this document is to set the requirements for a vulnerability management process based on a scan-prioritise-solve cycle in which we continuously check:

- how vulnerable our technical environment is to currently known vulnerabilities
- how our technical environment holds up to best practices
- set priorities based on the scan results and plan fixes or mitigating actions based on that priority.

We consider a vulnerability to be a weakness in a product or configuration, which allows an attacker to reduce a system's information assurance.
Scope for the document is to cover all KPN owned applications, devices or systems connected to an IP network (whether the network is a public one or a KPN one).

Version history

Version	*Date*	*Comments*
v1.0	3 September 2013	Approved in SSM
v1.1	11 October 2013	Updated based on consistency check
v2.0	27 March 2014	Updated references due to life cycle management
v2.1	15 April 2014	Update R03 to remove “critical” rating based on CVVS score
v2.2	15 October 2014	Version number incremented due to wrong number in CVSS table in Dutch policy version
v2.3	13 November 2015	Textual changes based on annual review
v2.4	5 February 2016	R01 explicated by pointing out that all interfaces must be scanned Editorial change in R03
v2.5	29 July 2016	R01: 'default' scanning of external interfaces explicitly mentioned R03: CVSS specified to CVSS v2 Base score
v2.6	3 February 2017	R01: Black zone specified further

ID	KSP-FA05-RL03-R01
Title	Vulnerability scanning
Description	Every KPN asset connected to a network must be scanned for vulnerabilities at least once per month with a vulnerability scanner. All interfaces of the asset must be scanned; including the logical and external interfaces. N.B.: 1. Customer assets hosted on the KPN network are excluded, as they are not KPN assets. 2. Vulnerability management on KPN assets connected to a black zone, not being internet or KOEN, may divert from this rule when other means of regular control of Vulnerabilities approved by KPN CISO is in place.
Relating document	Requirement: KSP-FA05-ST02-R08 (Vulnerability Management)

ID	KSP-FA05-RL03-R02
Title	Centrally managed vulnerability scanning
Description	The vulnerability scanning must be managed centrally for the whole of KPN, not by each segment individually. The owner and thus the segments must take appropriate measures to resolve the reported findings.
Relating document	Requirement: KSP-FA05-ST02-R08 (Vulnerability Management)

<table>
<tr><td>ID</td><td>KSP-FA05-RL03-R03</td></tr>
<tr><td>Title</td><td>Vulnerability mitigation</td></tr>
<tr><td>Description</td><td>Identified vulnerabilities (whether found based on the monthly vulnerability scanning, or found though other means) must be fixed according to the following timelines:

<table>
<tr><th>Category</th><th>CVSS v2 Base score*</th><th>Remediation time in case internet facing</th><th>Remediation time in case not internet facing</th></tr>
<tr><td>Low</td><td>0,0 - 3,9</td><td>Best effort</td><td>Best effort</td></tr>
<tr><td>Medium</td><td>4,0 - 6,9</td><td>1 month</td><td>2 months</td></tr>
<tr><td>High</td><td>7,0 - 10</td><td>2 weeks</td><td>1 month</td></tr>
</table>

If a vulnerability cannot be fixed, mitigating measures must be implemented according to the timeframe.

*Common Vulnerability Scoring System (CVSS) Score. Several vendors have their own definition of Low/Medium/High. To not be tied to a specific product or vendor, the categories are based on CVSS v2 Base scores. CVSS is a vulnerability scoring system designed by the Forum of Incident Response and Security Teams (FIRST) to provide an open and standardized method for rating IT vulnerabilities and is considered an industry standard for scoring vulnerabilities.</td></tr>
<tr><td>Relating document</td><td>Requirement: KSP-FA05-ST02-R08 (Vulnerability Management)</td></tr>
</table>