Overview of selected KPN Security Policies

Creation date: Wednesday, March 7, 2018 11:43:03 AM

Selected by: Ruud Leurs

Requirement	**Vulnerability scanning**
Description	All KPN assets connected to a network must, on atleast a monthly basis, be scanned for vulnerabilities by a vulnerability scanner. All interface, including the logical and external interfaces, must be scanned.
ID	KSP-RE-253
Version	1.0
Date	December 11, 2017
Rationale	Scanning of vulnerabilities (vulnerability management)

Requirement	**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.
ID	KSP-RE-254
Version	1.0
Date	December 11, 2017
Rationale	Scanning of vulnerabilities (vulnerability management)

<table>
<tr><td>Requirement</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.

Portal authority findings of CVSS 4.0 or higher need to be solved before go Live. (Portal authority base scores on CVSS v3)

*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 v3 in development.</td></tr>
<tr><td>ID</td><td>KSP-RE-255</td></tr>
<tr><td>Version</td><td>1.0</td></tr>
<tr><td>Date</td><td>December 11, 2017</td></tr>
<tr><td>Rationale</td><td>Scanning of vulnerabilities (vulnerability management)</td></tr>
</table>

Requirement	Updates
Description	Security updates must be installed per the timelines set in KSP-RE-255 (Vulnerability mitigation) on all KPN assets. This must be verified regularly. Deviations must be resolved as quickly as possible.
ID	KSP-RE-256
Version	1.0
Date	December 11, 2017
Rationale	Scanning of vulnerabilities (vulnerability management)

Requirement	**Vulnerability management**
Description	A vulnerability management process must be implemented and followed.
Supplement	Keeping security patch levels (as opposed to functional patch levels) up to date or implement mitigating measures minimizes the window of opportunity attackers have to exploit weaknesses for which patches or mitigating measures are available. Also factors like availability of support for specific software and patch levels should be taken into account here. It might occur that patches break the system; in such a case the vulnerability management process has been followed, but the requirement as is stated currently is not adhered to.
ID	KSP-RE-257
Version	1.0
Date	December 11, 2017
Rationale	Scanning of vulnerabilities (vulnerability management)

Requirement	**Vulnerability Management**
Description	Every system is to be scanned for vulnerabilities on a regular basis. The resulting findings need to be resolved within a pre-defined timeframe depending on the severity.
Supplement	Vulnerabilities can arise over time and must be solved timely to keep the system sufficient safe for attacks. i.e. Schedule of vulnerability tests for systems Isolated systems (without network link and no mobile storage applicable) have no need for vulnerability management.
ID	KSP-RE-258
Version	1.0
Date	December 11, 2017
Rationale	Scanning of vulnerabilities (vulnerability management)