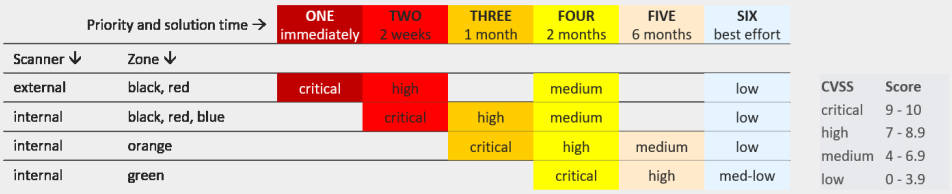
Overview of selected KPN Security Policies

Creation date: Thursday, May 9, 2019 4:08:00 PM

Selected by: Ruud Leurs

Requirement	**Vulnerability scanning**
Description	All KPN assets connected to a network, must be scanned for vulnerabilities on a minimum monthly basis. All interfaces, including the logical and external interfaces, must be scanned. The asset owner of the system on which the vulnerabilities have been found must take measures in response to the findings.
Supplement	Customers' assets that are part of the KPN network are not in scope for vulnerability scanning. Vulnerability management on KPN assets with an interface in a black zone, not being Internet or KOEN, may deviate from this rule if other, by CISO approved ways, regular management of vulnerabilities are met.
ID	KSP-RE-253
Version	1.1
Date	November 2, 2018
Rationale	Vulnerability scanning- and management

Requirement	**Centrally managed vulnerability scanning**
Description	Vulnerability scanning must be managed centrally and managed for the entire KPN organization.
ID	KSP-RE-254
Version	1.1
Date	November 2, 2018
Rationale	Vulnerability scanning- and management

Requirement	**Vulnerability mitigation**
Description	Identified vulnerabilities (whether found based on the monthly vulnerability scanning, or found through other means) must be fixed according to the following timelines:  If a vulnerability cannot be fixed, mitigating measures must be implemented according to the timeframe.
Supplement	**Categories of vulnerabilities** # External: Internet facing Vulnerabilities detected from an external scanner / the Internet. # Internal: not-Internet facing Vulnerabilities detected on the inside. **Scoring on** # CVSS version 3: critical, high, medium and low* # Zones: black, red, orange, green and blue * Common Vulnerability Scoring System (CVSS) Score. Several vendors have their own definition of Low/Medium/High/Critical. To not be tied to a specific product or vendor, the priorities are based on CVSS v3 Base scores.
ID	KSP-RE-255
Version	2.0
Date	February 20, 2019
Rationale	Vulnerability scanning- and management

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	Vulnerability scanning- and management

Requirement	**Vulnerability management process**
Description	A vulnerability management process must be implemented and followed.
ID	KSP-RE-257
Version	1.2
Date	May 3, 2019
Rationale	Vulnerability scanning- and 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	Vulnerability scanning- and management