Overview of selected KPN Security Policies

Creation date: Monday, May 13, 2019 10:58:38 AM

Selected by: Ruud Leurs

Requirement	**WiFi Protected Setup**
Description	No form of use of Wifi Protected Setup (WPS) is allowed.
ID	KSP-RE-420
Version	1.0
Date	December 11, 2017
Rationale	WLAN security

Requirement	**WLAN configuration and connectivity**
Description	When implementing a WLAN the following must be used: KPN WLAN with large user base (for example KPN Office Network) use wpa2-enterprise KPN managed client device must validate the authentication server based on certificate Users may access the KPN Office Network after authentication only when offered over the SSID KOEN_Wlan managed by KPN MijnWerkplek KPN WLAN with small user base, dedicated or personal scope: must be secured with WPA2 with minimal key of 16 characters distribute and keep access keys conform private key requirements the accessed network must be segmented from the KPN Office Network KPN CPE WLAN for business and residential: must be secured with WPA2 with minimal key of 16 characters initially the accessed network must be the on premise network of the customer
Related info	Example of implementation with windows: Microsoft's guide - Configure PEAP and EAP methods: http://technet.microsoft.com/en-us/library/cc784383(v=WS.10).aspx Client validation settings enforcement: http://technet.microsoft.com/en-us/library/cc759575(v=ws.10).aspx#cert_based
ID	KSP-RE-421
Version	1.1
Date	August 16, 2018
Rationale	WLAN security
Rationale	Security testing to innovation and development

Rationale	Authentication
Rationale	System hardening
Rationale	Registration of assets
Rationale	Cleaning of storage media
Rationale	Encrypting network traffic
Rationale	Data protection
Rationale	Cryptography generic
Rationale	Reporting security incidents

Requirement	**WiFi Direct**
Description	No form of use of Wifi-Direct is allowed.
ID	KSP-RE-419
Version	1.0
Date	December 11, 2017
Rationale	WLAN security

Requirement	**Wireless connectivity to control and maintain objects**
Description	It is forbidden to control or maintain any object used for services, service componentens, or applications (which include service platforms) using any type of wireless connectivity. This includes the security and safety related systems to these objects. Examples of forbidden wireless connectivity is: Wi-Fi Bluetooth Infra-red Mobile network Other radio-based solutions using any type of antenna NFC-based solution with a maximum usage of 20 centimeters or less from (virtual) card to reader is allowed.
Supplement	Radio based control and maintenance is susceptible to security, safety and continuity risks due to electro-magnetic disturbances and unable to control the object, man-in-the-middle attacks, circumvention of physical (access) controls and barriers due to radio leakage through walls.
ID	KSP-RE-754
Version	1.0
Date	May 3, 2019
Rationale	WLAN security
Rationale	Separating environments