

Friday, April 20, 2018 10:17:16 AM

Ruud Leurs

Requirement	Device (BYOD) lock-out
Description	<p>Device (BYOD) lock-out must be forced following multiple failed authentication attempts (after 10 incorrect passwords/PIN codes in succession).</p> <p>No connection to corporate infrastructure is possible anymore until it is determined that the device (BYOD) still is in possession of the registered owner.</p>
ID	KSP-RE-462
Version	1.0
Date	December 11, 2017
Rationale	BYOD (Bring Your Own Device)

Requirement	Device (BYOD) change or employment termination
Description	<p>When an employee with a device registered for use in the BYOD program changes to a new device or leaves the company:</p> <p>a) access to the corporate infrastructures must be revoked for the registered device(s) owned by the employee;</p> <p>b) the KPN data on the registered device must be wiped within 48 hours by using the de-registration script by the owner. The employee sends a confirmation email of this action to the KPN Security Helpdesk.</p>
ID	KSP-RE-463
Version	1.1
Date	April 4, 2018
Rationale	BYOD (Bring Your Own Device)

Requirement	Use of wireless keyboards
Description	<p>All forms of wireless use of a keyboard is not allowed.</p> <p>An exception is possible when the Bluetooth Passkey Entry is used to authenticate the keyboard with the host using a random PIN per pairing sequence. The exception is void when used for vital infrastructure maintenance.</p>
Related info	Guide to Bluetooth Security van NIST (Special Publication 800-121)
ID	KSP-RE-464
Version	1.0
Date	December 11, 2017
Rationale	BYOD (Bring Your Own Device)
Rationale	Security testing to innovation and development
Rationale	Authentication methods
Rationale	System hardening
Rationale	Registration of assets
Rationale	Cleaning of storage media
Rationale	Encrypting network traffic
Rationale	Data protection
Rationale	Reporting security incidents

Requirement	Mobile Device Management (MDM) software
Description	<p>Centrally provided Mobile Device Management (MDM) software must be installed, that provides remote:</p> <p>a) lock-out of the device;</p> <p>b) monitoring of device (BYOD) activity (in the event evidence is required for forensic analysis);</p> <p>c) deletion (often referred to as 'remote wipe') by securely destroying all KPN information stored on the device (BYOD) and any attached storage.</p>
ID	KSP-RE-695
Version	1.0
Date	April 4, 2018
Rationale	BYOD (Bring Your Own Device)