Overview of selected KPN Security Policies

Creation date: Monday, May 13, 2019 11:09:05 AM

Selected by: Ruud Leurs

Requirement	**Use of the SafeMail platform**
Description	All outgoing e-mail sent from the protected domains on Safemail must be handled by the Safemail platform.
Supplement	
Related info	
ID	KSP-RE-360
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform

Requirement	**Use of e-mail addresses**
Description	E-Mail communication from respectively KPN and Telfort must always use a sender-address in the @kpn.com or @telfort.com domain. The administrators of the Safemail platform choose which e-mailaddress is linked to which e-mail communication.
ID	KSP-RE-361
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform

Requirement	**Use of Domain Keys Identified Mail (DKIM)**
Description	All e-mail communication from the domain to be protected, must be signed with a DKIM key which is compliant to cipher suite- (KSP-RE-481) and key compromision requirements (KSP-RE-470).
Supplement	
Related info	
ID	KSP-RE-363
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**Use of Sender Policy Framework (SPF)**
Description	All legitimate e-mail communication from the domain to be protected must be relayed through a SMTP server, which is included in the SPF record of that domain.
Supplement	
Related info	
ID	KSP-RE-364
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**Use of Transport Layer Security (TLS) on a Mail eXchanger (MX)**
Description	The e-mail communication of KPN and subsidiaries must run through SMTP servers, which make use of opportunistic STARTTLS or better.
Supplement	A minimum of opportunistic STARTTLS is obliged to protect us against passive attackers (listeners) and minimize the impact on delivery of e-mail.
ID	KSP-RE-365
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**Reference in the e-mail body to a URL**
Description	All email towards KPN consumers must use URLs in its message body which are build-up from a hostname component which is within the kpn.com DNS zone. A (transparent) re-direct is allowed from a URL within the kpn.com DNS zone towards a page outside this zone. Good examples: www.kpn.com/invoices/ mijn.kpn.com/ zakelijk.kpn.com/some-particular-campagne/ Bad examples: campagnekpn.nl/ kpncampagne.nl/ facebook.com/kpncampagne/ youtu.be/kpn
ID	KSP-RE-366
Version	1.0
Date	December 11, 2017
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**Including an URL towards a login page**
Description	In e-mail communication from the @kpn.com domain towards customers the body of the e-mail message may never include an URL towards a direct login page. Example: When a customer is asked for an action in the ‘Mijn KPN’ environment, direct the customer towards kpn.com and explain the customer to login to ‘Mijn KPN’.
ID	KSP-RE-367
Version	1.0
Date	December 11, 2017
Rationale	Secure e-mail processing with a central platform

Requirement	**E-mail security**
Description	The owner of a service that sends out e-mail in the name of KPN or Telfort must ensure the service is connected to the SafeMail platform.
ID	KSP-RE-368
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**Mobile Mail for MSPs**
Description	Managed Service Providers may not receive emails from or containing information pertaining to KPN or her daughter companies on their mobile device(s).
ID	KSP-RE-369
Version	1.0
Date	December 11, 2017
Rationale	Secure e-mail processing with a central platform

Requirement	**Use of Secure/Multipurpose Internet Mail Extensions (S/MIME) certificate**
Description	E-mail communication to clients from a @kpn.com sender adress included in the corporate communications policy must be signed with an S/MIME certificate. The receiver of the message must be able to verify the authenticity and integrity of the e-mail.
Supplement	The corporate communications policy can be found in the KPN Brand Portal - https://www.kpnbrandportal.nl
ID	KSP-RE-362
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**Sending e-mail from a domain**
Description	Domains of KPN, subsidiaries or relevant suppliers that send e-mail, must be protected with a DMARC record, linked to a valid SPF and DKIM configuration for this domain. It is obligated to run a DMARC reject policy.
ID	KSP-RE-696
Version	1.1
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**DKIM Key Rotation**
Description	Every three months, the DKIM keys must be rotated. Old keys must be kept for 7 days.
ID	KSP-RE-745
Version	1.0
Date	February 1, 2019
Rationale	Authentication of e-mail
Rationale	Secure e-mail processing with a central platform

Requirement	**"Non-sending" domains**
Description	Domains in ownership of KPN and subsidiaries that do not fulfill a mailfunction, must be protected by a SPF and DMARC record with reject policy.
Supplement	When there are no protecting resource records on the domain, phishing campaigns can be run on the spoofable domain, which risks damaging KPN brand and consumers.
ID	KSP-RE-747
Version	1.0
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail

Requirement	**DKIM Selector Naming**
Description	DKIM Selector corresponds with sending server to identify and distinguish between these sending servers when DKIM signing occurs on multiple MTAs.
Supplement	The selector is sent within the mailheader to query the correct public key. If a false e-mail has been sent with a compromised key, this key and the compromised party must be traced through the false e-mail.
ID	KSP-RE-746
Version	1.0
Date	February 1, 2019
Rationale	Secure e-mail processing with a central platform
Rationale	Authentication of e-mail