Overview of selected KPN Security Policies

Creation date: Thursday, May 9, 2019 3:54:16 PM

Selected by: Ruud Leurs

Requirement	**Key Rollover**
Description	A ZSK rollover must happen every month. A KSK rollover must happen every 365 days.
Supplement	As the cryptographic material of a ZSK and KSK is often shared it reduces the strength of the key material. Therefore both keys need to be changed on a regular basis.
ID	KSP-RE-430
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	**NSEC3 hashing**
Description	The number of hashing iterations used for NSEC3 must be 2.
Supplement	Hashing used in NSEC3 does not provide a meaningful increase in security if the number of iterations is more than 2.
ID	KSP-RE-431
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	**Single-type key signing schemes**
Description	Single-type signing schemes are not allowed. The KSK or ZSK shall never be reused. Only 1 active KSK and ZSK is allowed per zone. Other ZKSs are and KSKs are allowed but only temporarily for the purpose of a key rollover.
Supplement	To reduce the operational impact of a ZSK or KSK rollover, unique keys are required.
ID	KSP-RE-432
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	**DNS Zone Transfer**
Description	Zone transfers that are not explicitly authorized via a written statement by the responsible KPN personnel or are not encrypted using KSP compliant algorithms are not allowed and shall be blocked.
Supplement	Zone transfers may contain sensitive information and shall therefore not be shared with entities outside of KPN to prevent the leakage of information
ID	KSP-RE-433
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	**Signing of domains**
Description	All DNS-domains that can be resolved via the internet and owned by or directly related to KPN, her Brands as determined by CIPO, or a daughter organization must be signed by DNSSEC.
Supplement	To be able to always guarantee the integrity of a DNS response sent by KPNs systems or received by KPNs customers DNSSEC must be used by all systems, applications, and domains owned by KPN which can be reached from the internet. This requires all domains of the KPN brand, or that of her daughters, to use this technique to secure their DNS responses. For example SPF, DKIM, DMARC, DANE, and CAA DNS records improve the security of Email and HTTPS connections however these records can be manipulated when sent via normal DNS message thereby mitigating the benefit these records provide. DNSSEC prevents this from happening by protecting the integrity of the DNS responses containing the records.
ID	KSP-RE-423
Version	1.2
Date	November 2, 2018
Rationale	DNS and DNSSEC

Requirement	**TLSA DNS records**
Description	KPN Systems using certificates for authentication, including but not limited to SMTP, must publish their certificate in a DNSSEC signed TLSA record.
Supplement	To increase the trust of the certificate supplied by a system (e.g. during setup of a HTTPS connection), the receiving system can verify it by resolving the system and getting a signed TLSA record. The TLSA record is also what is used for DANE.
ID	KSP-RE-434
Version	1.2
Date	August 16, 2018
Rationale	DNS and DNSSEC

Requirement	**Storage of DNSSEC keys**
Description	DNSSEC keys will always be stored in a HSM compliant with FIPS 140-2 security level 3 or higher.
Supplement	The DNSSEC keys are critical for delivering trustworthy domains to anyone who accesses the domains of owned, hosted, or managed by KPN. Loss or compromise of these keys must be prevented at all costs.
ID	KSP-RE-424
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	CAA DNS records
Description	Any internet-facing domain of KPN or daughter company that uses certificates must have a DNSSEC signed CAA record in their respective authoritative DNS platform. The email address 'abuse@kpn.com' must be used for the incident reporting field.
Supplement	To prevent a Certificate Authority from signing certificates that they are not authoritative for a CAA record is used to state the Certificate Authority authoritative for that domain. All CAs shall check, as per the 8th of September 2018 that a CAA record exists and shall only sign certificates they are allowed to. For the list of trusted CAs see KSP-RE-490 - you can find the link at the bottom of the page. Below you can find an example configuration with all trusted, used, and by CPO approved Certificate Authorities. If, within the domain, no certificates are used by one of the parties stated below then these parties must be removed from the configuration. kpn.com CAA 0 iodef "mailto:abuse@kpn.com" kpn.com CAA 0 issue "kpn.com" kpn.com CAA 0 issuewild "comodoca.com" kpn.com CAA 0 issue "geotrust.com" kpn.com CAA 0 issuewild "globalsign.com" kpn.com CAA 0 issue "comodoca.com" kpn.com CAA 0 issuewild "geotrust.com" kpn.com CAA 0 issue "globalsign.com" kpn.com CAA 0 issuewild "digicert.com" kpn.com CAA 0 issue “digicert.com" In the list above Amazon and Let's Encrypt certificates have not been included due to the free variant often being abused for phishing attacks and websites that host malware.
ID	KSP-RE-435

Version	1.5
Date	May 3, 2019
Rationale	DNS and DNSSEC

Requirement	**Third party resolvers**
Description	All recursive DNS traffic originating from a system owned by KPN, excluding customers, shall be handled by a DNS platform owned and managed by KPN. Recursive queries using a different DNS resolver as destination shall be dropped and logged. The logs must immediately be sent to a central logging entity as per KSP-RE-499.
Supplement	To prevent data exfiltration or leaking of information to third parties the use of 3rd party resolvers is not allowed.
ID	KSP-RE-436
Version	1.2
Date	August 16, 2018
Rationale	DNS and DNSSEC

Requirement	**Non-existing domains**
Description	To indicate that a domain does not exist, an NSEC3 record or better must be used.
Supplement	NSEC is a DNS record that indicates that a certain domain name does not exist on the server however it also leaks information on which domains do exist. NSEC3, the evolution of NSEC, prevents this by hashing the answer however rainbow tables allow the domain name to be retrieved. As some domain names need to be kept secret newer mechanisms, such as NSEC5, are being developed and should, with agreement of CISO, be used.
ID	KSP-RE-426
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	**DNSSEC resolving**
Description	All systems or applications owned by KPN that use DNS resolving must always resolve using DNSSEC. All DNS (stub)resolvers must indicate they are DNSSEC capable by resolving with the DO flag enabled.
Supplement	DNSSEC protects the integrity of a DNS answer. To be sure that the systems of KPN use this protection mechanism they need to let others know that they support DNSSEC as a feature. This indication is given by the (stub) resolver setting the D0 (D zero) flag in a DNS request. If the requested domain does not use DNSSEC then a normal DNS response will be sent.
ID	KSP-RE-427
Version	1.2
Date	November 2, 2018
Rationale	DNS and DNSSEC

Requirement	**DNSSEC algorithms**
Description	The cryptographic algorithms used for DNSSEC shall be compliant to the KSP. ED25519, algorithm #15, is preferred.
Supplement	Strong, future proof algorithms are also required for DNSSEC.
ID	KSP-RE-428
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	**NSEC3 Salt**
Description	If NSEC3 is used a random salt of 8 bytes shall be used. This salt shall be automatically regenerated when a ZSK key-rollover takes place.
Supplement	To prevent an attacker from finding the hashed domain names stored in an NSEC3 record a random, as per FA05-RL07-R01, salt shall be used. To reduce the effectiveness of an attack the salt shall be changed regularly.
ID	KSP-RE-429
Version	1.1
Date	June 18, 2018
Rationale	DNS and DNSSEC

Requirement	**DNS Exfiltration**
Description	DNS resolvers must be able to detect and block any attempts at using the DNS protocol for the exfiltration of data from networks or systems of KPN or subsidiaries. All detected and/or blocked events must be logged and sent to a central logging server.
Supplement	An attacker wanting to get data out of a network or system wants to do that in a manner so that they are not detected. By encoding the data into a DNS request, for example in the domain field (eW91IGdldCBhIGNvb2tpZQ==.baddomain.ng) an attacker can make it seems like valid DNS traffic, get it out of the victims network, and receive it at the domains authoritative DNS server that they control. A mechanism to prevent this from happening needs to be in place to be able to detect, and prevent, this from happening. For example, by detecting that a system is sending tens of DNS resolve messages to the same domain (baddomain.ng), and blocking and logging the event.
ID	KSP-RE-698
Version	1.0
Date	June 18, 2018
Rationale	DNS and DNSSEC