DFN-PKI

Interne Namen in Serverzertifikaten in der DFN-PKI

- Sicherheitsniveau Global -

1 Problembeschreibung

In der DFN-PKI ist es im Sicherheitsniveau Global nur noch bis 2015 möglich, interne Namen oder reservierte IP-Adressen in Serverzertifikaten zu verwenden. Danach ist dies im Sicherheitsniveau Global nicht mehr möglich. Auch von allen anderen im Browser vorinstallierten öffentlich vertrauten PKIs wie z.B. von Verisign oder Comodo sind solche Zertifikate dann nicht mehr erhältlich.

Interne Namen meint Namen im Common Name oder im Subject Alternative Name in Serverzertifikaten, die nicht in einer Top Level Domain liegen, die in der IANA Root Zone registriert sind, und damit nicht im öffentlichen DNS verifizierbar global eindeutig sind.

Ein Beispiel für einen internen Namen ist „mail.local". Auch Namen ohne jeden Domain-Anteil wie z.B. „mail" werden hier als interne Namen bezeichnet.

Reservierte IP-Adressen meint IP-Adressen, die von der IANA explizit als reserviert bezeichnet werden, und die an der folgenden Stelle aufgelistet werden:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Ein Beispiel für eine reservierte IP-Adresse ist 192.168.6.1

Interne Namen und reservierte IP-Adressen sind in Zertifikaten einer öffentlich vertrauten PKI wie der DFN-PKI problematisch, da keine globale Eindeutigkeit gegeben ist. Ein interner Name „mail.local" kann in mehreren Einrichtungen verwendet werden und bezeichnet dann natürlich unterschiedliche technische Systeme. Wenn es jetzt ein Zertifikat in der DFN-PKI mit „mail.local" gibt, welches konkrete System aus welcher Einrichtung wird dann damit bezeichnet?

Aus diesem Grund hat das CA/Browser-Forum in den durch die DFN-PKI verpflichtend einzuhaltenden Baseline Requirements festgelegt, dass jetzt neu ausgestellte Serverzertifikat mit internen Namen oder reservierten IP-Adressen nur noch eine Laufzeit bis November 2015 haben dürfen. Am 1.10.2016 müssen alle noch gültigen betroffenen Zertifikate, die eventuell früher mit einer deutlich längeren Laufzeit ausgestellt wurden, gesperrt werden.

Eine ausführliche Beschreibung des Problems vom CA/Browser-Forum finden Sie unter:
https://cabforum.org/wp-content/uploads/Guidance-Deprecated-Internal-Names.pdf

2 Neue gTLDs

Bekanntlich schließt die ICANN zur Zeit Nutzungsverträge für mehr als 1000 neue gTLDs ab. Es ist nicht auszuschließen, dass dabei neue gTLDs entstehen, die von Organisationen bereits als

vermeintlich nutzbare interne Domains verwendet werden.

Die DFN-PCA wird nach Abschluss eines neuen gTLD-Vertrages von der ICANN informiert, und muss innerhalb von 30 Tagen prüfen, ob in der DFN-PKI Global Serverzertifikate existieren, die diese neuen gTLDs als vermeintlich interne Namen verwenden. Nach 120 Tagen nach Abschluss des Vertrages müssen diese Zertifikate gesperrt werden, es sei denn, der Zertifikatinhaber ist in der Lage, die Domain vom neuen Betreiber der gTLD zu kaufen.

Weitere Informationen hierzu finden Sie unter: https://cabforum.org/internal-names/

3 Migration von internen Namen

Wenn auf den Systemen, die bisher über interne Namen oder reservierte IP-Adressen, weiterhin browserverankerte Zertifikate aus der DFN-PKI Global oder von anderen Anbietern eingesetzt werden müssen, ist es erforderlich, diese umzubenennen bzw. mit öffentlichen IP-Adressen auszustatten.

Es ist dabei nicht erforderlich, dass jeder Servernamen im öffentlichen DNS auflöst, allerdings muss jeder Servername unterhalb einer Domain ausgestellt werden, die der Zertifikatinhaber entweder laut Whois oder nach einem Domain-Authorisierungsschreiben kontrolliert.

Beispiel: Die Einrichtung Hochschule Musterstadt hat einen Mailserver, der ausschließlich im internen Netzwerk erreichbar ist unter dem Namen „mail.local". Damit dieser Server auch weiterhin mit einem Zertifikat aus einer öffentlichen, in der Anwendungssoftware vorinstallierten PKI ausgestattet werden kann, muss er umbenannt werden in mail.hs-musterstadt.de

Einige Einrichtungen betreiben getrennte DNS-Server für externe und und einrichtungsinterne Namensauflösung. Es ist nicht erforderlich, dass Namen in Serverzertifikaten im externen DNS auflösen.

Möchte man die bisherigen internen Namen nicht in die vorhandene öffentliche Domain umziehen, bietet es sich an, eine weitere Domain nur für die ehemals internen Namen zu betreiben. Dies kann entweder als Subdomain unter der existierenden Domain, z.B. internal.hs-musterstadt.de, oder als eigenständige registrierte Domain wie z.B. hs-musterstadt-internal.de geschehen.

4 Ausstellung von Zertifikaten mit internen Namen oder reservierten IP-Adressen nach 2015

Ist eine Umbenennung nicht möglich, bleibt nur der Weg, Zertifikate aus nicht öffentlich vertrauten, nicht im Browser vorinstallierten PKIs einzusetzen. Hierfür gibt es prinzipiell drei Möglichkeiten.

4.1 Nutzung einer DFN-PKI Internal CA

In der DFN-PKI wird eine spezielle Zertifizierungsstelle, die ohne Policy betrieben wird, keinem Audit unterliegt und nicht im Browser verankert ist, mit der Serverzertifikate mit internen Namen oder reservierten IP-Adressen ausgestellt werden können.

Wenden Sie sich an dfnpca@dfn-cert.de, wenn sie diese Möglichkeit nutzen wollen.

Beachten Sie, dass Sie das DFN-PKI Internal CA Zertifikat an alle Nutzer, die auf einen Server mit einem entsprechenden Zertifikat zugreifen wollen, bekannt machen müssen.

4.2 Aufbau einer Einrichtungs-eigenen internen PKI

Eine andere Möglichkeit ist der Aufbau einer eigenen PKI in der Einrichtung. Insbesondere in einer Microsoft Active Directory Umgebung gibt es eine relativ einfach einzurichtende CA-Umgebung, mit der teilweise sogar Auto-Enrollment-Szenarien umgesetzt werden können. In einer entsprechenden Umgebung kann das selbst-signierte CA-Zertifikat auch automatisch auf die Klienten ausgerollt werden.

4.3 Nutzung von einzelnen Selbst-signierten Zertifikaten

Sind nur wenige, einzelne Server betroffen, die nicht von vielen Nutzern verwendet werden, kann für jeden einzelnen Server ein selbst-signiertes Serverzertifikat erstellt und eingesetzt werden. Man spart sich hierbei den Aufwand des PKI-Betriebes, muss aber mit besonderer Sorgfalt die jeweiligen Serverzertifikate bei den Nutzern bekannt machen.

Diese Variante ist nur bei wenigen Servern, die von technische erfahrenen Nutzern verwendet werden, zu empfehlen.

5 Spezialfälle

Für Microsoft Exchange mit Outlook 2007 Autodiscovery waren in der Vergangenheit teilweise Zertifikate mit einfachen Hostnamen notwendig. Dabei wurde der NetBIOS-Name des Servers in das Zertifikat geschrieben. Eine Umstellung auf ein Zertifikat mit dem voll qualifizierten Domain-Namen des Exchange-Servers gibt unter Umständen Fehlermeldungen auf den Outlook-Clients. Mit folgender Anleitung lässt sich das Problem beheben: http://support.microsoft.com/kb/940726