Prüfbericht des LA Governikus

Mit der Entscheidung 2014/24 "Weiterentwicklung Verbindungsnetz" hat der IT-Planungsrat folgenden Beschluss getroffen:
1. Der IT-Planungsrat bittet das Arbeitsgremium Verbindungsnetz und den Bund, für den Datenaustausch zwischen Ländern (einschließlich Kommunen) ohne Beteiligung des Bundes gemeinsam eine tragfähige Position zur Umsetzung des §3 IT-NetzG zu erarbeiten.
2. Der IT Planungsrat bittet den Lenkungsausschuss „Governikus“ zu prüfen, ob die Anwendung „Governikus“ um Komponenten eines Sicherheitsgateways erweitert werden kann, dass der sichere Betrieb der OSCI-Intermediäre sowohl in verwaltungseigenen Netzen als auch im Internet gewährleistet ist.

Prüfbericht zu Zf. 2 der o. g. Entscheidung

Der Datenaustausch zwischen dem Bund und den Ländern erfolgt über das Verbindungsnetz, welches die informationstechnischen Netze des Bundes und der Länder verbindet. Die Netze des Bundes und der Länder können zudem Übergänge zum Internet haben, die gemäß der einschlägigen Empfehlungen des BSI abgesichert sein müssen. Die Kommunikationspartner (Fachliche Sender/Empfänger) und deren OSCI-Intermediäre können daher sowohl über das Verbindungsnetz und das jeweilige Landesnetz, als auch über das Internet erreichbar sein.

Absicherung der Intermediäre auf Netzebene

Die Anwendung „Governikus“ des IT-Planungsrats stellt im Sinne der OSCI-Infrastruktur die Funktionalität eines Intermediärs zur Verfügung. Dieser ist auf Netzebene von einem direkten Zugriff zu entkoppeln. Für den Dateneingang aus dem Internet und aus dem Verbindungsnetz/Landesnetz kommen jeweils Reverse-Proxies zum Einsatz. Diese terminieren den Datenstrom und leiten ihn intern an die entsprechenden Systeme (eventuell mit Loadbalancer Funktion) weiter. Darüber hinaus sollen die Reverse-Proxies als Applikationsgateway (s. u.) dienen, um dezidierte Freigaben zu ermöglichen.

Abbildung 1 zeigt ein Beispiel für die Verortung eines Intermediärs innerhalb der DMZ. Denkbar ist auch die Bereitstellung des Intermediärs in anderen, sicheren Netzsegmenten (z.B. Intranet).

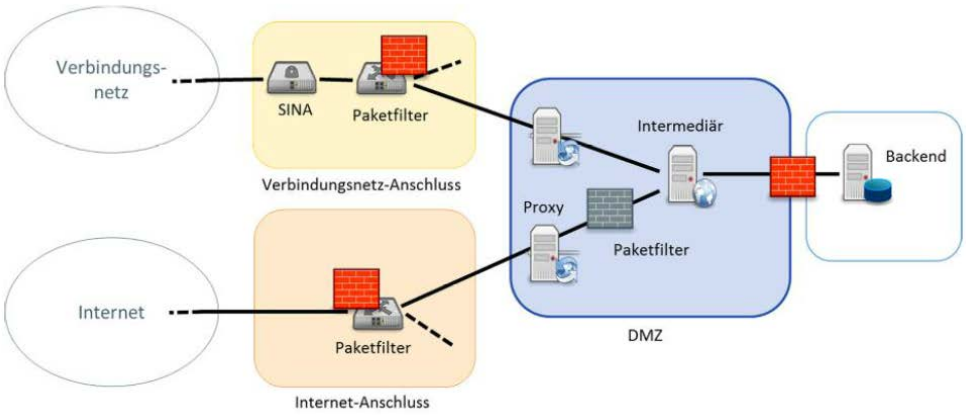

Abbildung 1: Dedizierter Schutz eines „zweibeinig angeschlossenen“ Intermediärs (Quelle: Übergang der vom IT-NetzG betroffenen Kommunikationsbeziehungen auf das Verbindungsnetz, Version 0.9)

Der Betrieb eines OSCI-Intermediäres für die Bund-Länder-Kommunikation muss den Anschlussbedingungen des (künftigen) Verbindungsnetzes genügen. Nach derzeitigem Stand muss ein zugelassenes Sicherheitsgateway bzw. ein Securitysystem, bestehend aus Paketfiltern und Applikationgateways gemäß der BSI-Leitlinie „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA) / BSI-Leitlinie zur Internet-Sicherheit (ISi-L)“ eingesetzt werden.

Im laufenden Betrieb der Anwendung Governikus muss für die Zertifikatsprüfung eine Verbindung ins Internet zu den Prüfadressen der Zertifikatsdiensteanbieter aufgebaut werden können. Diese Kommunikation wird über den XKMS-Standard realisiert. Dieser Standard beschreibt eine spezielle XML-Struktur, in der Prüfinformationen (z.B. von X-509-Zertifikaten) übermittelt werden können. Für diese Verbindung kann ein zentral konfigurierter Proxy zum Einsatz kommen. Hierfür ist die BSI-Leitlinie „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA) / BSI-Leitlinie zur Internet-Sicherheit (ISi-L)“ einschlägig. Diese ist in der Anwendung Governikus bereits umgesetzt, so dass keine technischen Änderungen erforderlich sind.

Änderungen an der Anwendung Governikus

1. Für den Einsatz in synchronen Szenarien müssen zukünftig für die einzelnen Empfänger jeweils die Adressen der – je nach Netzzugang – unterschiedlichen Proxyserver konfiguriert werden können. Hierzu sind u.a. Erweiterungen in der Administrationsanwendung von Governikus erforderlich.
2. Bestehende Anweisungen zum Betrieb der Anwendung sind um Hinweise zur Konfiguration mit Reverse-Proxies und einem Sicherheitsgateway zu erweitern.

Der Lenkungsausschuss Governikus stellt fest, dass zur Gewährleistung des sicheren Betriebs sowohl in verwaltungseigenen Netzen als auch im Internet lediglich geringfügige technische Änderungen an der Anwendung Governikus erforderlich sind. Die vorgenannten Änderungen können kostenneutral im Rahmen von Change Requests für die Anwendung Governikus umgesetzt werden.

Änderungen an Fachverfahren / Transportverfahren

OSCI-Datenübermittlungen zwischen verschiedenen Bundesländern bzw. mit dem Bund sind bisher fast ausschließlich über das Internet erfolgt. Durch das IT-NetzG ist ein zusätzlicher Weg eröffnet worden. Dies ist unproblematisch, sofern sich aus den Rechtsvorschriften eindeutig ergibt, welches Netz gewählt werden muss. Es wird aber viele Fälle geben, in denen beide Alternativen zulässig sind, also sowohl die Nutzung des Internet als auch des Verbindungsnetzes.

Vor jeder Datenübermittlung müssen die zum Zeitpunkt des Versendens einer OSCI-Nachricht gültigen Kommunikationsparameter aus Verzeichnisdiensten bezogen werden. Verzeichnisdienste sind das DVDV (Deutsches Verwaltungs- und Dienste Verzeichnis) sowie SAFE für den elektronischen Rechtsverkehr. Die vom Verzeichnisdienst gelieferten Kommunikationsparameter enthalten die Informationen für eine Versendung der OSCI-Nachricht über das Internet als auch über das DOI-Netz (zukünftig Verbindungsnetz), welche derzeit optional sind. Auf Grund der fast ausschließlichen Versendung von OSCI-Nachrichten über das Internet seit Beginn des DVDV im Jahre 2007 ist davon auszugehen, dass die gängigen Implementierungen der Fachverfahrenssoftware in Bund und Ländern derzeit **keine** Funktion zur Auswahl der Netze für die Versendung von OSCI-Nachrichten zur Verfügung stellen.

FAZIT

Die Anwendung „Governikus“ kann um Komponenten eines Sicherheitsgateways erweitert werden, so dass der sichere Betrieb der OSCI-Intermediäre sowohl in verwaltungseigenen Netzen als auch im Internet gewährleistet ist. Die dafür erforderlichen Aktivitäten können im Rahmen der Pflege der Anwendung kostenneutral umgesetzt werden.

Der Lenkungsausschuss Governikus stellt fest, dass eine entsprechende Erweiterung der Anwendung Governikus dazu beiträgt, die Zielsetzung des IT-Netzgesetzes optimal zu unterstützen. Die bei Bund, Ländern und Kommunen betriebene Anwendung kann neben den bereits bestehenden Datenübermittlungen zukünftig auch für die gemäß § 3 IT-NetzG über das Verbindungsnetz erfolgenden Datenübermittlungen zwischen dem Bund und den Ländern genutzt werden.

Der Lenkungsausschuss Governikus weist darauf hin, dass Anpassungen an den Fachverfahren bzw. den Transportverfahren erforderlich sein werden, um die von den Verzeichnisdiensten zukünftig übermittelten Verbindungsangaben für das Verbindungsnetz korrekt umzusetzen. Die Änderungen werden komplexer, sofern Verzeichnisdienste zukünftig alternative Übermittlungswege anbieten werden, zwischen denen eine Auswahl zu treffen ist.

Kurzbeschreibung der notwendigen Change Requests an den LA Governikus zu Abstimmung:

Change Request 1: „Erweiterungen der Governikus-Komponente Backend-Enabler für das Versenden von Nachrichten in unterschiedliche Netze“

Für den Einsatz in synchronen Szenarien müssen zukünftig für die einzelnen Recipients jeweils die Adressen der – je nach Netzzugang – unterschiedlichen Proxyserver konfiguriert werden können. Hierzu sind u.a. Erweiterungen in der Administrationsanwendung von Governikus erforderlich.

Change Request 2: „Erweiterung der Governikus-Dokumentation im Hinblick auf die Einhaltung der Einsatzbedingungen für das Verbindungsnetz“

Die Dokumente „Governikus Installationshandbuch“ und „Governikus Betriebshandbuch“ sind dahingehend zu erweitern, dass dort für die Betreiber von Governikus-Intermediären alle im Hinblick auf die Einsatzbedingungen für den Anschluss an das Verbindungsnetz notwendigen Mechanismen (u.a. Paketfilter, ALG, Proxy-Server, Angriffserkennungserkennungssoftware (IDS/IPS), Schutz vor DDoS-Angriffen) beschrieben werden.