Die wahre Dimension der Anpassung der Netzwerke und IT-Infrastruktur für die Ärzte und andere Leistungserbringer, verursacht durch die fortgeschrittene Gefährdungslage im Internet und Anbindung an die Telematikinfrastruktur per VPN

In der Stellungnahme zu den Musterschreiben von MEDI GENO bezüglich des TI-Konnektors (Aktuelles) vom 17.07.2019 wird erläutert (Zitat aus öffentlicher Meldung):

Installation und Betrieb des Konnektors

Die Ausstattung bzw. der Anschluss der medizinischen Einrichtungen an die TI liegen außerhalb des Verantwortungsbereiches der gematik und erfolgen durch die jeweiligen IT-Dienstleister der Leistungserbringer. Dies betrifft insbesondere den Konnektor.

Eine sach- und fachgerechte Installation der Anbindung an die TI durch den DVO/AIS-Dienstleister setzt daher grundsätzlich die Einhaltung der Hinweise und Dokumente des Bundesamtes für Sicherheit in der Informationstechnik und der gematik voraus.

siehe

https://www.gematik.de/news/news/stellungnahme-zu-den-musterschreiben-von-medi-geno-bezueglich-des-ti-konnektors-1/

Die Voraussetzungen finden sich also direkt beim BSI, dem Bundesamt für Informationssicherheit.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet bereits seit vielen Jahren Informationen und Hilfestellungen rund um das Thema IT-Sicherheit: Die IT-Grundschutz-Kataloge des BSI sind inzwischen zum umfassendsten Standardwerk zur IT-Sicherheit geworden. Siehe z.B.

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html

Die Sammlung umfasst mit Einleitung und Katalogen über 4.800 Seiten und dient Unternehmen und Behörden als Grundlage zum Erlangen einer Zertifizierung nach IT-Grundschutz . (aus Wikipedia)

https://de.wikipedia.org/wiki/IT-Grundschutz-Kataloge

Als weitere Quelle sind die Hinweise und Dokumente der gematik zu berücksichtigen!

z.B. für die Dienstleister vor Ort, siehe Titel und Dokument:

Anschluss medizinischer Einrichtungen an die Telematikinfrastruktur –
Ein Überblick für Dienstleister vor Ort (DVO)

https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Service/Anschluss_medizinischer_Einrichtungen_an_die_Tele-matikinfrastruktur__DVO_/gemInfo_Anschluss_TI_DVO_V2.2.0_Anh.pdf

In diesem Dokument befindet sich dann der Hinweis auf eine weitere Informations-Quelle, siehe:

https://www.gematik.de/mediathek/publikationen/

Alles in allem geht es um viele 1000 Seiten die durchzulesen sind um dann eine geeignete Auswahl zu treffen, welche der Informationen und Vorgaben zwingend zu berücksichtigten sind.

Niemand hat bisher extrahiert welche Vorgaben in Frage kommen!

Die Anbindung an ein bestehendes Arzt-Netzwerk, bzw. an die bestehende EDV-Infrastruktur, wird bestimmt vom Konnektor und vom gewählten Zugangsverfahren einer VPN-Verbindung (VirtualPrivate Network).

Lassen wir im Moment ausser acht, dass es verschiedene VPN-Arten gibt, z.B. konventionelles VPN und SSL-VPN und dass der Konnektor als Sonderkonstruktion möglicherweise aus dem Rahmen fällt, schauen wir nur einmal nach den grundlegenden Standards und Arbeitsschritten, die berücksichtigt werden sollen.

Einen ersten Aufschluss gibt der Abschnitt NET_3_3_VPN des BSI, siehe

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_3_VPN.html

hier mit einigen ausgewählten Anforderungen zur Nutzung von VPN:

(Zitatfrei aus amtlichem Werk entnommen):

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein VPN. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.3.3.A6 Durchführung einer VPN-Anforderungsanalyse

Es SOLLTE eine Anforderungsanalyse durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigte Hard- und Software-Komponenten ableiten zu können. In der Anforderungsanalyse
SOLLTEN folgende Punkte betrachtet werden:

Geschäftsprozesse,
Zugriffswege,
Identifikations- und Authentisierungsverfahren,
Benutzer und Benutzerberechtigungen,
Zuständigkeiten und
Meldewege.

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein VPN vorrangig umgesetzt werden:

Vor der Einführung eines VPN MUSS eine sorgfältige Planung erfolgen. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MUSS regelmäßig kontrolliert werden, ob der VPN-Dienstleister die vereinbaren Sicherheitsmaßnahmen einhält.

Das zugrundeliegende Betriebssystem der VPN-Plattform MUSS sicher konfiguriert werden. Wird eine Firewall-Appliance benutzt, MUSS es dafür einen gültigen Wartungsvertrag geben. Es MUSS sichergestellt werden, dass nur qualifiziertes Personal VPN-Komponenten installiert.

Die Installation der VPN-Komponenten sowie eventuelle Abweichungen von den Planungsvorgaben SOLLTEN dokumentiert werden. Die Funktionalität und die gewählten Sicherheitsmechanismen des VPN MÜSSEN vor Inbetriebnahme geprüft werden. Für VPN-Clients, VPN-Server und VPN-Verbindungen MUSS eine sichere Konfiguration festgelegt werden.

Diese SOLLTE geeignet dokumentiert werden. Auch MUSS der zuständige Administrator regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

Zusammengefasst ergeben sich daraus folgende Schritte und Aufwände *:

- Vorplanung
- VPN-Anforderungsanalyse > bedeutet IST-Analyse des Arztnetzwerkes, bzw.
- der vorliegenden EDV/IT-Infrastruktur
- SOLL-Anforderungen ermitteln (z.B Hardware, Software, Organisation verändern, Supportkosten, Kostenermittlung u.vm.
- Einsatz einer Firewall-Appliance
- Dokumentation
- Vorprüfung Inbetriebnahme
- Laufende Kontrolle/Monitoring

An dieser Stelle muss ein großes AHA einsetzen, die Erkenntnis, dass das gematik-Konzept der Aufstellung des Konnektors und die angebotenen Anschlussarten nicht mit den Anforderungen* des BSI zusammenpassen. Die Unterschiede sind derart gravierend, dass man sich fragen muss wer die Erlaubnis gegeben hat dieses informationelle System auszurollen, ohne diese Punkte zu berücksichtigen und abzuarbeiten.

Kein Wunder das katastrophale Entwicklungen bei den Installationen und der Inbetriebnahme eingetreten sind.

Aus meiner Sicht und der vieler anderer Systemadministratoren, die intensiv mit Netzwerkanalysen und Migrationen, also der Umstellung von IT-Systemen auf einen erweiterten Zustand, befasst sind, ist die Umsetzung des größten informationellen Systems der Welt, der eGK und Telematikifrastruktur, vollkommen unzureichend.

Und dies ist eine höfliche Umschreibung.

Ein wesentlicher kritischer Faktor ist auch dadurch gegeben, dass die Konnektor und Systemanbindung per Gesetz erzwungen wird.

Ohne Rücksicht auf die bestehenden Situationen und Anforderungen wird der Konnektor und die Telematikinfrastruktur-Anbindung auf sehr unterschiedliche Infrastrukturen 'aufgepropft'.

Die Pressemeldung wird zur Farce mit der Aufforderung, man solle die Vorgaben des BSI berücksichtigen, denn diese Vorgaben beziehen sich ebenso auf die gematik selbst, die diese nicht erfüllt hat und noch viel schlimmer nie erfüllen kann.

Die Konsequenz der Erfüllung der genannten Schritte und Aufwände * würde bedeuten, dass die gematik, bzw. deren beauftragte Dienstleister, sich umfassend in die bestehende Netzwerksituation der Ärzte und anderer Leistungserbringer einarbeiten um in gemeinsamen Maßnahmen, in einer gegenseitigen vertrauensvollen Verbindung mit hoher Transparenz, den bestmöglichsten Systemzustand herzustellen.

Das die KBV nun an einer IT-Sicherheitsrichtlinie arbeitet und erkennt, dass hier hohe zeitliche und finanzielle Aufwände zu erwarten sind ist sicher gut gemeint, zeigt aber auch wie wenig die Kassen und Verbände von den wahren technischen Bedingungen und Sachverhalten wissen (siehe https://www.aend.de/article/201512).

Die KBV kann sicherlich eine Richtlinie erarbeiten, in irgendeiner Form, diese wird aber niemals eine auf die Kernpunkte des BSI heruntergebrochene Richtlinie sein können und sie kann auch nicht die unüberbrückbaren Systemfehler aus der Welt schaffen.

Die Diskrepanz aufzulösen ginge theoretisch nur dann, wenn das Konzept und die Umsetzung des eGK/TI-Systems stark verändert wird, was seinem Ende gleichkommen würde.

In diesem Zusammenhang war eine der fehlerhaftesten Aussagen immer die, dass die Verantwortung am Konnektor enden kann.

Es gibt kein Ende und auch keinen Anfang in einem vertrauensvollen VPN-Netzwerk, es ist stets ein gemeinsames Netzwerk mit vielen Wegen und Toren (nicht-linear).

Von Anfang an war die Idee private nicht-staatliche Teilnehmer zwangsweise per VPN an ein Industrie-Netzwerk anzubinden ein beispielsloser Akt in der Geschichte der Einflussnahme der Industrie auf Politik und das Parlament.

In politischer und demokratischer Hinsicht ist einer der größten Brüche dadurch entstanden, einen VPN-Tunnel in jedes private Netzwerk zu erzwingen, um anschließend Zugriff auf die Software-Systeme und Daten zu erhalten.

Was auch spektakulär ist sind die tatsächlichen Kosten, die mit einer Erfüllung der Vorgaben der gematik und des BSI verbunden sind! Denn diese High-End Anforderungen, in einem sagen wir -hochprofessionellem Umfeld - treffen auf kleinste IT/EDV Infrastrukturen, bzw. sehr unterschiedliche Systemsituationen, wie z.B. Arztpraxen ohne Internetanschluss.

Auch die Einführung und der Betrieb einer Firewall-Appliance in den gegebenen Umständen erfordert ein hohes fachliches Können, auch wenn die Anschaffungs-, Support- und Replacement-Kosten bei wenigen tausend Euro liegen.

Das erste Problem sind die Migrationsanforderungen und deren Kosten, so kann es sein, dass die Ermittlung der IST-Situation dazu führt, dass weitere IT-Spezialisten hinzugezogen werden müssen oder die komplette Hardware- und Software erneuert werden muss und das zweite Problem sind die Folgekosten, je nach Größe des angebundenen Netzwerkes.

Und wenn wir die Zahl der ca. 200 000 Leistungserbringer berücksichtigen, die an die Telematikinfrastruktur angeschlossen werden sollen, dann brauchen wir natürlich dafür auch die 200 000 hochqualifizierte IT-Fachkräfte (zertifiziert), die die Anforderungen der gematik und des BSI erfüllen und das Ganze in Zukunft begleiten.

Was bleibt ist eine lange Liste an Anforderungen, die nicht abgearbeitet worden sind. Niemand hat vorher ermittelt, mit einer ausreichenden Anzahl an Testverfahren, wie teuer die Anbindung für die Leistungserbringer werden kann.

Dadurch das 200 000 eigentlich bisher dezentrale Systeme zusammen vernetzt werden über ein einziges informationelles System wurde die Angriffsfläche extrem vergrößert. 200 000 dezentrale Systeme können über Viren kompromittiert werden, aber sie können nur mit sehr großen Aufwand separiert werden.

Nun ist die Rede also davon Richtlinien und Lösungen zu schaffen, doch wieviel Zeit wird für echte Lösungen benötigt und was kommt dabei raus wenn diese Lösungen erprobt werden? Zumal schon jetzt erkennbar ist, dass die Richtlinien des BSI stark von der Systemwirklichkeit der Telemtikinfrastruktur abweichen!

Besser wäre es gewesen als erstes die Richtlinien für die Verbesserung der Sicherheit der Leistungserbringer zu entwickeln und danach zu schauen welche telematischen Lösungen für das Gesundheitssystem geeignet sind.

Hier noch ein abschließender Hinweis auf die Anforderungen, die mit IT-System-Migrationen zusammenhängen.

Siehe: Anleitung zur Migration von Sicherheitskonzepten Hilfsmittel zum modernisierten IT-Grundschutz. Referenzwerk für die IT-Sicherheit in Deutschland

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/Migrationsleitfaden/Anleitung_zur_Migration_node.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Anleitung_zur_Migration.pdf?__blob=publicationFile&v=10

Rolf D. Lenkewitz
Systemadministrator
Bergstraße 6
87769 Oberrieden
0163 170 68 09

Hinweise zu § 51 Urheberrechtsgesetz - Zitate:

Die markierten Zitate stammen aus öffentlichen Quellen, aus einer Pressemeldung der gematik und von den Webseiten des BSI und sind als amtliches Werk einzustufen, was den Bürger und Unternehmen frei zur Verfügung gestellt wurde. Ich verbreite daher öffentlich verfügbares Wissen in Zitaten mit dem Ziel komplexe Sachverhalte und inhaltliche Beziehungen aufzudecken, damit das System der elektronischen Gesundheitskarte und Telematikinfrastruktur und dessen Folgen besser eingeschätzt werden können.

Bitte beachten Sie als ergänzende Informationen:

http://www.rdlenkewitz.eu/DSGVO/dsgvo.html