EIN HOCHSICHERER VPN-ZUGANGSDIENST FÜR DAS GESAMTE GESUNDHEITSWESEN

GENUA Der Aufbau der Telematikinfrastruktur gilt als das größte IT-Projekt im Gesundheitsbereich. Sie vernetzt Ärzte, Apotheken, Krankenhäuser und Krankenkassen und schafft in Deutschland den Zugriff auf die Gesundheitsdaten von 70 Millionen gesetzlich Versicherten. Angesichts der hochsensiblen Daten ist es auch ein großes IT-Security-Projekt. Der Aufbau des ersten zugelassenen VPN-Zugangsdienstes zeigt, welche besonderen Herausforderungen gelöst werden mussten.

Laut gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) werden rund 70 Millionen gesetzlich Versicherte, 180 000 niedergelassene Ärzte und Zahnärzte, 20 500 Apotheken, 2 000 Krankenhäuser und 118 Krankenkassen die Telematikinfrastruktur (TI) nutzen. „Seit November 2017 befindet sich die Telematikinfrastruktur im Produktivbetrieb. Der reguläre Betrieb folgt auf eine dreijährige Erprobungsphase einschließlich einer langjährigen Zulassungsphase für eine Vielzahl sicherheitsrelevanter Komponenten“, erläutert Arthur Steinel, General Manager im Geschäftsbereich TELEMED der CompuGroup Medical Deutschland AG. Als Projektleiter für den VPN-Zugangsdienst, einer zentralen Komponente der TI, hat er einen tiefen Einblick in das gesamte Projekt.

SICHERE TELEMATIKINFRASTRUKTUR

Die TI ist ein geschlossenes Netz auf der Basis eines VPN-Zugangsdienstes (Virtual Private Network), zu dem nur registrierte Nutzer Zugang erhalten. Zu den Sicherheitsanforderungen gehörte der Aufbau eines gegenüber dem Internet abgeschotteten VPN-Netzes. Dabei erfolgt die sichere Authentifizierung der Teilnehmer beispielsweise in einer Arztpraxis auf Basis von Chipkarten (Praxis- bzw. Institutionskarte). Sie kommunizieren über einen sogenannten Konnektor, einem VPN-Router mit fest eingebauter Chipkarte.

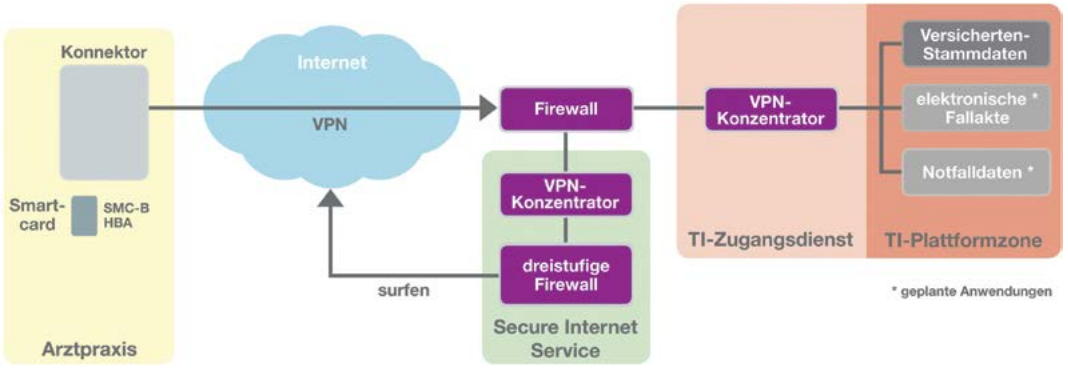
Die TI-Plattform liefert die Infrastruktur und stellt darauf aufbauende grundlegende Sicherheitsfunktionen zur Verfügung. Die wichtigsten Elemente sind:

- sichere, verschlüsselte Kommunikation und Schutz vor dem Zugriff auf sensible Informationen,
- gesicherte Authentisierung der Kommunikationspartner,
- Nutzung einer qualifizierten elektronischen Signatur,
- die verwendeten kryptographischen Verfahren werden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelmäßig überprüft und an die neuesten Entwicklungen angepasst,
- ein Datenschutz- und Informationssicherheitsmanagementsystem (DSMS/ISMS) überwacht den datenschutzkonformen und sicheren Betrieb der TI.

EIN FLÄCHENDECKENDER VPN-ZUGANGSDIENST FÜR DAS GESUNDHEITSWESEN

„Von der gematik als Zulassungsbehörde werden an einen flächendeckenden VPN-Zugangsdienst sehr hohe Anforderungen an die Funktionalität und Sicherheit gestellt“, berichtet Arthur Steinel. Um an der Erprobungsphase des VPN-Zugangsdienstes teilnehmen zu können, mussten die zentralen Hochsicherheitskomponenten, Firewalls und VPN-Konzentratoren, eine Zertifizierung durch das BSI auf der Basis von Schutzprofilen nach Common Criteria (CC) für IT-Produkte nachweisen. Mit den Schutzprofilen setzt das BSI Mindeststandards für ausgewählte Produktgruppen wie Netzwerk- und Kommunikationsprodukte. „Die Lösungen des deutschen IT-Sicherheitsherstellers genua GmbH, die vom BSI regelmäßig zertifiziert werden, erfüllen diese hohen Anforderungen“, so Steinel.

genua ist ein deutscher IT-Sicherheitshersteller mit Sitz in Kirchheim bei München. Als zentrale Firewall sowie als VPN-Konzentrator wird die Firewall&VPN-Appliance genuscreen eingesetzt. genuscreen ist eine hochwertige IT-Sicherheitslösung mit CC EAL 4+ Zertifizierung und Zulassung bis zur Geheimhaltungsstufe VS-NfD. Physisch getrennt von der sonstigen Telematikinfrastruktur erhalten die Teilnehmer mit dem „Secure Internet Service“ (SIS) einen extra abgesicherten Internetzugang. Der Projektleiter bezeichnet die dafür genutzte dreistufige Firewall als eine weitere wichtige Sicherheitskomponente. Das BSI empfiehlt zur Sicherung von Datennetzen mit mittlerem oder hohem Schutzbedarf den Einsatz mehrstufiger Firewall-Lösungen, die sich aus unterschiedlichen Systemen zusammensetzen. Die Firewall genugate besteht aus einem Application Level Gateway und einem Paketfilter und



Die Hochsicherheitskomponenten des VPN-Netzes verfügen über ein zertifiziertes CC-Schutzprofil mit kryptographischer Absicherung. „Die Lösungen des deutschen IT-Sicherheitsherstellers genua GmbH, die vom BSI regelmäßig zertifiziert werden, erfüllen diese hohen Anforderungen", berichtet Arthur Steinel, Projektleiter für den VPN-Zugangsdienst.

bietet somit bereits zwei Stufen. Dieses Konzept hat auch das BSI überzeugt, das die genugate mehrfach nach CC in der Stufe EAL 4+ zertifiziert hat. Dabei wurde stets der starke Widerstand gegen direkte Angriffe hervorgehoben. Hier erfüllt die genugate als einzige Firewall weltweit die CC-Anforderungen der Stufe EAL 7.

Die Firewall genugate, kombiniert mit einem weiteren Paketfilter, ergibt die angestrebte dreistufige Sicherheitslösung. Die drei Firewalls sind in Reihe geschaltet: Zunächst prüft ein Paketfilter (PFL) die Daten auf der Netzwerk- und Transportschicht-Ebene. Dann folgt das Application Level Gateway (ALG) auf der Anwendungsebene. Als dritte Stufe folgt ein weiterer Paketfilter, den die Daten bei ihrem Weg durch das gesamte Firewall-System durchlaufen müssen.

„Die Komponenten des VPN-Zugangsdienstes mussten schließlich in Hunderten von Tests nachweisen, dass sie die funktionalen und sicherheitstechnischen Anforderungen der Produktsteckbriefe tatsächlich erfüllten", erklärt der Projektleiter. Die Anforderungen für den VPN-Zugangsdienst umfassten allein über 300 Seiten. Und je Anforderung musste ein Testnachweis erbracht werden.

ZAHLREICHE HÜRDEN BEIM AUFBAU DER TELEMATIK-INFRASTRUKTUR

„In einem so großen Sicherheitsnetz mit sehr vielen Teilnehmern und höchst sensiblen Anwendungen ist die höchstmögliche Verfügbarkeit der Systeme eine kritische Anforderung. Deshalb werden alle Systeme in hochverfügbaren Clustern eingesetzt. Zusätzlich steht im Rechenzentrum für jedes Cluster ein Ersatz-System und das gleiche nochmals in einem räumlich getrennten Zweit-Rechenzentrum", so der Projektleiter. Fällt eine Komponente aus, steht nur eine kurze Zeit zur Verfügung, in der der Schwenk auf die Ersatzkomponente erfolgt sein muss.

„Wir hatten in der Anfangsphase als Betreiber einer essenziellen Komponente der TI als kritische Infrastruktur (KRITIS) gemäß des IT-Sicherheitsgesetzes eine meldepflichtige Notfallsituation durch einen Stromausfall an einem Internethauptknoten. Beim Wechsel zum Ausweichrechenzentrum gab es unerwartete Schwierigkeiten mit Komponenten. Hier haben die Spezialisten von genua zur entscheidenden Lösung beigetragen", gibt Steinel einen Einblick. Durch den gleichzeitigen Zugriff sehr vieler Konnektoren war eine Überlastsituation entstanden, die manuell behoben werden musste. Die Techniker von genua entwickelten daraufhin eine Lösung, die nun in ähnlichen Situationen einen automatischen Schwenk sicherstellt.

HOCHSICHERHEITSKOMPONENTEN HABEN SICH BEWÄHRT

Der Projektleiter des VPN-Zugangsdienstes zieht aus den Erfahrungen mit den eingesetzten Sicherheitskomponenten ein durchweg positives Fazit: „Mit dem Beginn des Produktivbetriebs bieten wir den VPN-Zugangsdienst im freien Wettbewerb an. Eine Zertifizierung der Komponenten nach dem BSI-Schutzprofil wird jetzt nicht mehr verlangt. Nach den sehr guten Erfahrungen mit den Komponenten von genua halten wir aber daran fest. Das hat sich bestens bewährt." Er verweist auch auf gute Erfahrungen mit dem Support des deutschen Herstellers. Entgegen der sonstigen Philosophie habe man hier kein eigenes Know-how zusätzlich aufgebaut, sondern vertraue auf die gute Beratung durch die Spezialisten von genua.
Als besonderen Nutzen der Lösung sieht er, dass die Technik speziell für sehr hohe Sicherheitsanforderungen konzipiert ist. „Das sind fertige Appliances mit abgestimmten Hardware- und Software-Komponenten. Sicherheit und Funktionalität sind für die erhöhten Anforderungen bereits optimiert. Da bringt das Unternehmen genua viel Erfahrung mit", zieht der Projektleiter sein Fazit.

genua Ein Unternehmen der Bundesdruckerei

GENUA GMBH
Domagkstraße 7, 85551 Kirchheim bei München
Tel.: +49-(0)89 991950-0
E-Mail: info@genua.de
www.genua.de

GRAFIK: © GENUA