Segeberger Kliniken

Ausgefeilte Sicherheit für zwei Netze

Im Gesundheitsbereich gelten bereits naturgemäß hohe Sicherheitsstandards. Da aber auch in Kliniken vermehrt vernetzte IT zum Einsatz kommt, müssen die Verantwortlichen dort ihre Sicherheitskonzepte in die nächste Ausbaustufe bringen. Sehr gut gelungen ist dies den Segeberger Kliniken - dank des ARP-GUARD der Hagener ISL, den der Sicherheitsdienstleister LargeNet aus Hamburg, als langjähriger Partner des Krankenhauses, implementierte.

Es ist keineswegs weit hergeholt, wenn das renommierte Magazin „CIO“ schreibt, dass IT-Sicherheit im Gesundheitswesen mehr bedeutet als Geschäftserfolg, sondern dass es dabei auch um „Leben und Tod“ geht. Und das gilt nicht allein für die Sicherheit der medizintechnischen Geräte, sondern auch für die der allgemeinen IT, die in Krankenhäusern immer mehr zum Einsatz kommt – beispielsweise für die kabellose Visite mittels Tablet-PC und WLAN-Anbindung. „Der ARP-GUARD kontrolliert neben den kabelgebundenen Geräten ebenfalls die Zugriffsberechtigungen der kabellosen Geräte, hier mit dem Standard 802.1X. Diese Flexibilität bietet längst nicht jedes Tool“, so Netzwerkprofi Marco Koch, System Engineer IT-Security bei LargeNet. „Die erfassten Patientendaten sind für uns das höchste Gut. Es muss von vornherein kategorisch ausgeschlossen sein, dass unberechtigte Zugriffe auf diese Daten möglich sind“, ergänzt Andreas Griese, IT-Leiter der SEGEBERGER KLINIKEN GMBH.

Andreas Griese
IT-Leiter der
SEGEBERGER
KLINIKEN GMBH

"... das medizinische und das allgemeine IT-Netz strikt voneinander trennen"

Das Unternehmen zählt zu den größten privat geführten Krankenhausunternehmen in Schleswig-Holstein und ist Arbeitgeber für mehr als 1.600 Mitarbeiterinnen und Mitarbeiter aus der Region. Mit insgesamt knapp 1.000 Betten bieten die Segeberger Kliniken für Patienten ein medizinisch ganzheitliches Leistungsangebot, bestehend aus Akutmedizin, Prävention, Rehabilitation und Pflege. „Und in diesem Konzept setzen wir stark auf die Unterstützung durch eine leistungsfähige IT“, so Andreas Griese.

Innovative Netzwerktechnologie - die geschützt sein will

In Zahlen ausgedrückt: In den Kliniken verrichten rund 920 PCs, mehr als 100 vernetzte medizinische Geräte und über 330 Drucker ihren Dienst. Ebenso werkeln dort 52 Datenverteiler, die mehr als 3200 mögliche Datenanschlüsse gewährleisten. Zudem ist in den einzelnen Gebäuden ein controllerbasiertes WLAN mit mehr als 400 Access Points für die Patientenvisite implementiert – für die Bad Segeberger eine stattliche Menge an Geräten, auch wenn diese Zahl gestandenen IT-Chefs, die nicht aus der Gesundheitsbranche stammen, womöglich nur ein müdes Lächeln aufs Gesicht zaubert. Warum dieses Konstrukt indes in Wirklichkeit höchst komplex ist, erläutert der IT-Leiter: „Aus gesetzlichen Gründen und aus Gründen der Patientensicherheit müssen das medizinische und das allgemeine IT-Netz strikt voneinander getrennt arbeiten“, so Andreas Griese. Das bedeutet: Es ist vollkommen ausgeschlossen, dass – auch nicht etwa versehentlich – ein medizinisches Gerät im allgemeinen Netz betrieben wird und umgekehrt.

Matthias Knörich
Geschäftsführender
Gesellschafter der
Hamburger
LargeNet GmbH

"... manuelle Sicherheitsvorkehrungen nicht mehr zeitgemäß"

Segeberger Kliniken

Automatische Sicherung statt „Handarbeit“

Vor der Implementierung des ARP-GUARD verließ sich das Unternehmen deshalb zur Sicherung seines Netzes primär auf bauliche Maßnahmen und manuelle Sicherheitsvorkehrungen, „allerdings kamen wir gemeinsam schnell zu dem Schluss, dass dieses Konzept nicht mehr ganz zeitgemäß war und wir im positiven Sinne aufrüsten mussten“, berichtet Matthias Knörich, Geschäftsführender Gesellschafter der Hamburger LargeNet GmbH, einem Unternehmen, das sich darauf spezialisiert hat, IT-Systeme vor inneren und äußeren Angriffen zu schützen.

Gemeinsam mit dem Klinikum haben sich Herr Knörich und sein Team aus guten Gründen für den ARP-GUARD der Hagener ISL GmbH entschieden, ein besonders wirksames System zum Aufbau eines aktiven Schutzschildes gegen fremde Geräte und interne Angriffe. Damit schließen Unternehmen eine Sicherheitslücke, die übliche Methoden wie Firewalls, Virenschutz oder Intrusion-Detection-Systeme nicht abdecken. Im Detail: Der ARP-GUARD durchsucht selbsttätig das Netzwerk nach Geräten, indem er mit den darin enthaltenen Routern und Switches kommuniziert. Wichtig: Der ARP-GUARD ist dabei in der Lage, mit allen gängigen Geräten zu kommunizieren, so dass Administratoren schnell einen Überblick über alle angeschlossenen Geräte erhalten. Herkömmliche Bestandslisten für den Netzwerkschutz sind meistens schnell veraltet. Zudem ist die übliche Vorgehensweise, bei der das IT-Personal händisch einzelne Geräte an bestimmten Ports zulässt, mit einem erheblichen Aufwand verbunden. Darüber hinaus erkennt ARP-GUARD sämtliche Geräte in heterogenen Switch-Umgebungen; dem Administrator entgeht also nichts.

Umfangreiche Funktionalität deutlicher Pluspunkt

Ein weiterer Vorteil des Netzwerkwächters sind dessen Funktionalitäten im Virtual Local Area Network (VLAN). Dieses virtualisierte Netz ist ein logisches Teilnetz innerhalb eines Switches oder eines gesamten physischen Netzwerks, das heißt ein physisches Netzwerk wird in mehrere kleine Netzwerke aufgeteilt. Es kann sich über einen oder mehrere Switches hinweg ausdehnen. Laienhaft ausgedrückt: Mittels VLAN lässt sich ein „echter“ Switch beispielsweise in fünf virtuelle verwandeln. Das VLAN trennt also physische Netze in Teilnetze auf. „Und der ARP-GUARD ist selbsttätig in der Lage, die Ports der Switche in die entsprechenden VLANs zu distribuieren, je nach MAC-Adresse des angeschlossenen Geräts“, so Marco Koch. Andreas Griese ergänzt: „Dies vereinfacht uns natürlich das Netzwerkmanagement und das vernetzte Arbeiten insgesamt, da der ARP-GUARD die Clients aktiv in das VLAN verschiebt und parallel die Autorisierung übernimmt.“ Sprich: Der ARP-GUARD sorgt automatisiert dafür, dass die Geräte in das zugehörige VLAN geschoben werden. Ein händisches Eingreifen ist nicht mehr notwendig, mögliche Fehlerquellen sind ausgeschlossen und administrative Eingriffe, beispielsweise bei Umzügen, sind nicht mehr notwendig. Gleiches gilt für die Genehmigung länger nicht mehr genutzter Geräte: Auch hier ist der ARP-GUARD fähig, eine aktive Rolle zu übernehmen und bei Bedarf den Zugang zum Netz zu versperren.

Fazit:

Die Segeberger Kliniken haben mit dem ARP-GUARD eine leistungsfähige, kostengünstige und flexible Möglichkeit gefunden, ihre Netzwerksicherheit stark zu erweitern. Zudem hat der norddeutsche Gesundheitsbetrieb dadurch mehr Komfort für die Administration bekommen und kann schließlich auch seine Services ausbauen. Darüber hinaus haben die Kliniken mit der Implementierung bereits heute eine wichtige Maßnahme eingeleitet, die in naher Zukunft auch andere Krankenhäuser intensiv beschäftigen wird: Auf europäischer Ebene erarbeitete neue Normen werden für die IT und die Medizintechnik in den Krankenhäusern voraussichtlich schon bald massive Auswirkungen haben. Die von den Vorschriften geforderten Prozesse werden, vor allem in der Netzwerktechnik, für Krankenhäuser erhebliche Eingriffe bedeuten, „die wir uns aber werden sparen können, da wir mit dem ARP-GUARD in dieser Hinsicht bereits vorgesorgt haben“, resümiert Andreas Griese.