IT+Technik

SCHOTTEN **DICHT**!

In diesem Beitrag geht es darum, wie man ungebetene Gäste fernhält und Netze mit unterschiedlichen Sicherheitsanforderungen – auf nur einem Switch – betreiben kann.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Die Möglichkeiten zur Absicherung eines Netzwerkes sind vielfältig und unterscheiden sich (partiell) in der Zielsetzung. Bei der Segmentierung von Netzwerken unterbindet bzw. kontrolliert man den Datenaustausch zwischen zwei Netzen mit unterschiedlichen Aufgaben und dementsprechend variierendem Schutzbedarf (z.B. Netzwerk mit Patientendaten und Netzwerk zum Internetsurfen während der Mittagspause).
Eine de facto zwingend erforderliche Segmentierung ist der Schutz und damit die Abgrenzung Ihres (Praxis-)Netzwerks gegen das Internet – über eine dedizierte Firewall oder über die in einem Router enthaltene Schutzfunktion.
Die Realisierung einer Netztrennung innerhalb der Praxis kann physikalisch oder virtuell erfolgen. Bei der physischen Trennung haben Sie zwei Netzwerke, die für sich autark bestehen und die – wenn überhaupt – über eine Firewall miteinander verbunden sind. Hier regelt die Firewall wie beim Internetübergang auch, welche Verbindungen in welche Richtung und mit welchem Inhalt (bspw. über Festlegung von Protokollen) erlaubt sind. Dank immer leistungsfähigerer Netzwerk-Controller können Sie heutzutage aber auch zwei oder mehr Netzwerke mit nur einem physischen Switch realisieren und sogenannte VLANs (Virtual Local Area Network) aufsetzen.
Ungeachtet der gewählten Implementierung erreichen Sie somit, dass Ihre AIS/PVS Systeme mit sensiblen Informationen nicht aus dem anderen Netzsegment erreicht werden können. Auch der Internetübergang kann restriktiver eingestellt und Protokollierung aktiviert werden. Im hiervon separierten Netzwerk (genutzt bspw. als reine Internet-Arbeitsplätze oder für Tests) sind die Schutzvorkehrungen geringer, dafür aber jegliche Patientendaten verboten.
Eine anders gelagerte Zielsetzung verfolgen Sie, wenn Sie in einem Netzwerk nur erwünschte (i.e. autorisierte) Endgeräte an der Kommunikation zulassen wollen. Denn indem Sie unerwünschte Netzteilnehmer von vorne herein ausschließen, reduzieren Sie das Risiko des ungewünschten Datenabflusses, da angeschlossene Netzwerk-Komponenten aktiv ausgeschlossen werden und ein Angriff auf das Netzwerk so bereits im Ansatz unterbunden wird.

Lösungen hierzu werden in der Regel als „Network Access Control"-Tools bezeichnet und arbeiten mit unterschiedlichen Techniken. Die reine Filterung auf Ebene von „MAC-Adressen" (Media-Access-Control) lässt nur im Vorhinein registrierte Netzwerkkomponenten zu, kann aber durch einen motivierten Angreifer umgangen werden. Weiterführende Lösungen ergänzen dies durch logische Prüfungen, z.B. Abschaltung von Anschlüssen, wenn durch Ausprobieren die gemeldeten Adressen sehr schnell wechseln (sogenanntes „Spoofing").

DNS - Das „Domain-Name-System"

Wie an dieser Stelle in der letzten Ausgabe beschrieben, wird spätestens mit der Einführung von IPv6 die Lesbarkeit von IP-Adressen durch den Menschen völlig unpraktikabel – aber bereits heute möchte sich kein normaler Anwender IP-Adressen im Format „195.137.170.128" merken. Daher wurde bereits früh ein System entwickelt, welches – im Hintergrund – sprechende Namen wie www.hausaerzteverband.de in die zugehörige, eindeutige IP-Adresse übersetzt und so die Kommunikation ermöglicht.

Foto: fotolia