KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

STANDARD FÜR FIREWALLS IN PRAXEN

In diesem Dokument wird beschrieben, welcher Schutz bzgl. dem Internetzugang von Praxen empfehlenswert ist. Dabei wird als erstes auf Services eingegangen die vorhanden sein sollten, danach auf spezielle Firewalls, die diese Services bieten.
Der Kontext liegt auf der Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit von der Kassenärztlichen Bundesvereinigung.
https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf

SCHUTZZIELE IM RAHMEN DIESES DOKUMENTS

Das Dokument beschreibt den Zugang einer Praxis ins Internet, bzw. den Zugriff von außen auf eine vertragsärztliche oder vertragspsychotherapeutische Praxis.

Hierfür wird ein Standard zum Einsatz einer Firewall beschrieben, sofern eine Praxis einen direkten Zugang zum Internet besitzt.

ZUGANG VON DER PRAXIS INS INTERNET

Der Schutz von der Praxis ins Internet ist dann erforderlich, wenn ein direkter Zugang zum Internet existiert. Das ist beispielsweise bei einem parallelen Betrieb des Konnektors[1] im Netzwerk der Praxis der Fall. Soll der Zugang zum Internet abgesichert werden, empfiehlt es sich den Konnektor im Reihenbetrieb zu installieren. Damit schützt die TI bzw. der Sichere Internetservice (SIS) des VPN-Zugangsdienstanbieters das Netzwerk der Praxis. Im Reihenbetrieb kann auch eine sogenannte stateless Firewall verwendet werden, die jegliche Verbindung zum Internet (ausgenommen die Verbindung vom Konnektor ins Internet) unterbindet. Die Funktionalität dafür wird meistens von den Routern, welche schon im Einsatz sind, zur Verfügung gestellt.

Soll eine direkte Anbindung an das Internet von der Praxis möglich sein, ist eine Firewall zum Schutz des Praxisnetzes empfehlenswert. Die Firewall sollte folgende Schutzmechanismen bieten:

- die Möglichkeit einer physischen und/oder logischen (VLAN) Netzwerkseparierung in verschiedene Sicherheitszonenzwecks Netzwerksegmentierung
- Paketfilter, der Quelle, Ziel, Port und Protokoll unterscheiden kann
- Protokollierung von administrativen und kritischen Ereignissen
  - Systemänderungen
  - erkannte bösartige Zugriffsversuche
- Alarmierung bei kritischen Ereignissen
- Vorhandene Wartung: für die gesamte Laufzeit der Firewall müssen Sicherheitsupdates zur Verfügung stehen
- URL-/Web -Filter: Schutz vor Zugriffen auf bekannte, bösartige Domains und IPs
- Extension blocking: Schutz vor dem Download von ungewollten, ausführbaren Dateien (empfehlenswert, aber nicht notwendig)

---

[1]Informationen zu dem unterschiedlichen Betriebsarten des Konnektors (parallel, reihe/ seriell etc.) gibt die gematik unter https://fachportal.gematik.de/fileadmin/Fachportal/Leistungserbringer/Informationsblatt_Betriebsarten-Konnektor_V1.0.0.pdf

› Malwarescanner: Kontrolle auf bekannte Viren bei Downloads und Zugriffen
› Intrusion Prevention System (IPS): Erkennen und blockieren von Angriffen

Möglicherweise vorhandene Gastnetze, die Besuchern zur Verfügung gestellt werden, sollten immer von dem internen Netz getrennt werden.

ZUGANG VOM INTERNET IN DIE PRAXIS

Zu schützen ist unter anderem der Zugang aus dem Internet in die Praxis. Dieser Schutz wird meist durch den Router generiert, indem dieser keine Verbindungen von außen zulässt. Der Schutz mit Hilfe des Routers wird nicht gewährleistet, wenn zum einen ein Dienst der Praxis im Internet verfügbar ist (der Dienst muss dabei in dem Praxisnetzwerk gehostet werden und vom Internet aus erreichbar sein wie eine Praxis-Homepage oder eine Online-Terminvereinbarung), oder wenn Internet of Things (IoT) Geräte wie IP Kameras im Netzwerk der Praxis beispielsweise über IPv6 im Internet verfügbar sind. In diesem Fall werden die IPv6 Adressen im lokalen Netzwerk, welche die Praxis als Kunde vom ISP[2] erhält, direkt und ohne Schutz durchgereicht. Der Schutz des NATings[3] (Transformieren einer öffentlichen IPV4 Adresse in eine interne IPV4 Adresse entfällt). Darüber hinaus kann es auch zu ungewollten Freigaben von Ordnern, Dateien, Druckern oder sonstigen z.B. per Universal Plug and Play (UpnP) verbundenen Geräten kommen, wenn diese ungewollt oder irrtümlich nach außen freigegeben werden. Ein weiterer Zugriff von außen auf das Netz kann durch Fernwartung erfolgen, dieser Zugriff sollte temporär und auf berechtigte Teilnehmer der Wartungsfirma beschränkt werden. Ist in diesem Sinne mindestens ein Service im Internet verfügbar, sollte das Praxisnetzwerk mit einer dedizierten Firewall (vgl. Tabelle 1) geschützt werden.

WELCHE FIREWALL FÜR WELCHE PRAXIS?

Wenn eine Firewall alle diese genannten Schutzmechanismen enthält und fachgerecht konfiguriert und betrieben wird, ist das Netzwerk weitestgehend vor bösartigen Netzwerkverbindungen geschützt. Zu beachten ist, dass diese Schutzmechanismen kein Garant für unerwünschte Zugriffe sind. Eine Schulung in der beispielsweise auf bösartige Mails eingegangen wird, ist ergänzend zu den Mechanismen zu sehen.

Im Folgenden sind Beispiele für Firewalls aufgezeigt, welche die genannten Schutzmechanismen unterstützen:

Hersteller und Modell	Kosten für Hardware	Kosten für Hardware und ergänzende Sicherheitsfunktionen / Updates (1. Jahr)	Jährliche Folgekosten	Max. Unternehmensgröße
Zyxel USG 40	374,68 €	466,00 €	unbekannt	kleine Unternehmen
FortiNet FortiGate 30E	383,00 €	632,00 €	350, 00€	kleine Unternehmen
Cisco Firepower 1010	567,45 €	Unbekannt	unbekannt	kleine Unternehmen

Tabelle 1: Beispiel für Firewalls mit Kosten und Unternehmensgröße. Alle Preise ggf. zzgl. MwSt. und zzgl. weitere Kosten für Installation und Wartung

Die angegebenen Preise können zum einen abweichen, zum anderen ist darauf zu achten, dass die Hardware nur mit dem Kauf einer zusätzlichen Wartungslizenz den vollen Umfang zur Verfügung stellt. Ohne diese Lizenzen können meist nur grundlegende Dienste, wie der Paketfilter genutzt werden. Somit

[3] NAT: Network Address Translation

muss mit initialen und laufenden Kosten gerechnet werden. Außerdem ist darauf zu achten, dass der Support für die jeweilige Hardware vom Hersteller während der Nutzungszeit nicht eingestellt wird.
Der Funktionsumfang der Firewall ist nicht von der Anzahl der Mitarbeiter abhängig, sondern von der benötigten Datendurchsatzrate. Da jede Firewall nur einen definierten Datendurchsatz verarbeiten kann, welcher von der Leistungsfähigkeit der verbauten Hardware abhängig ist, muss der maximale Datendurchsatz bei der Beschaffung berücksichtigt und eine ausreichend skalierte Firewall angeschafft werden. Kleine Unternehmen im Kontext dieses Dokuments sind alle Unternehmen welche bis zu 20 Mitarbeiter haben. Es ist davon auszugehen, dass eine Praxis hauptsächlich lokal arbeitet und der Durchsatz zum Internet pro Mitarbeiter, im Vergleich zu einem Unternehmen gleicher Größe in anderen Branchen, geringer ist. Deshalb können die zuvor genannten Firewalls auch noch bei mehr als 20 Mitarbeitern eingesetzt werden. Wenn signifikant mehr Mitarbeiter in einer Praxis arbeiten, können die in Tabelle 1 benannten Geräte auch in stärkeren Ausführungen erworben werden.

Es sind auch unabhängig von der TI sogenannte Sichere Internetservice (SIS) Lösungen am Markt erhältlich. Betreiben zentral leistungsfähige Firewalls und bieten die oben beschriebenen Schutzmechanismen einer Firewall für Endkunden an. Die Praxis verbindet sich in der Regel über eine verschlüsselte VPN-Verbindung zu dem SIS-Anbieter, der die Firewall betreibt. Vor der Beauftragung einer solchen Lösung sollte allerdings nachfragt werden welche Schutzmechanismen der einzelne Anbieter in dem konkreten Angebot auch realisiert.

Die in den meisten Routern integrierte Firewall kann in der Regel nicht alle der oben beschriebenen Schutzmechanismen anbieten.