Schweizerische
Fachschule

TEKO

Fallstudie IT-Sicherheit

Sicherheitskonzept für die Arztpraxis

Verfasser:
Christian Rybovic

Studiengang:
Dipl. Informatiker HF

Klasse:
L-TIP-24-Do-a

Webseite:
neo.christianrybovic.ch

Datum der Abgabe:
5. März 2026

Management Summary

Die Praxis verfügt über eine funktionierende IT-Infrastruktur. Allerdings bestehen mehrere Sicherheitslücken, insbesondere im Bereich der Netzwerkstruktur. Über WLAN, ungeschützten Zugriff auf kritische Netzwerkkomponenten und zu geringe Sicherheitsmassnahmen im Netzwerk, gibt es ein breites Spektrum für mögliche Angriffe.

Ein Angriff könnte den Praxisbetrieb mehrere Tage lahmlegen. Patientendaten könnten verloren gehen oder veröffentlicht werden. Neben finanziellen Schäden drohen ein erheblicher Vertrauensverlust und mehrere gerichtliche Auseinandersetzungen.

Um die Angriffsfläche zu reduzieren und den Schutz sensibler Daten nachhaltig zu verbessern, werden in diesem Dokument auf Basis einer Risikoanalyse verschiedene Massnahmen vorgeschlagen. Einige Massnahmen lassen sich durch entsprechende Konfigurationen umsetzen, während andere mit zusätzlichem finanziellem und organisatorischem Aufwand verbunden sind.

Inhaltsverzeichnis

1.Ausgangslage

Die Arztpraxis verfügt über eine klassische Sterntopologie, wobei alle Geräte direkt oder indirekt mit dem Router verbunden sind. Es ist keine Netzwerksegmentierung erkennbar und kritische Geräte (Röntgengerät und Drucker) sind über WLAN mit dem Netzwerk verbunden. Die nachfolgende Grafik zeigt eine Möglichkeit des Netzwerkaufbaus, wie er in der Arztpraxis umgesetzt sein könnte:

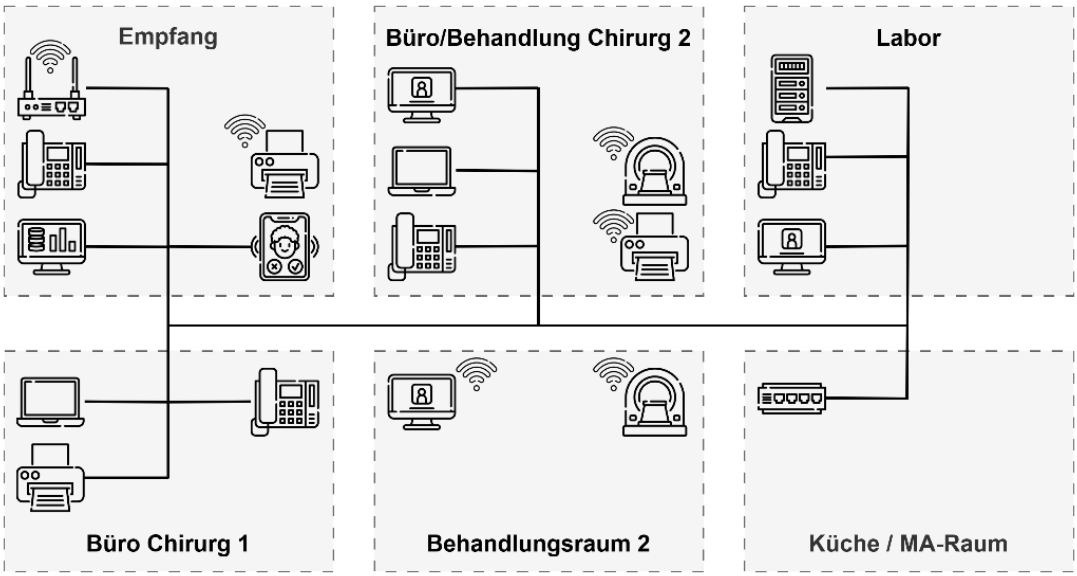

Abbildung 1: Netzwerktopologie Arztpraxis

2.Abgrenzung

Nicht Bestandteil dieser Arbeit sind die konkrete Arbeitsweise der Mitarbeiter, organisatorische Abläufe und interne Prozesse sowie die detaillierte Betrachtung der eingesetzten medizinischen oder administrativen Softwarelösungen. Darüber hinaus werden keine technischen Konfigurationsanleitungen (Client-/Servereinstellungen, Firewall-Konfigurationen, usw.) ausgearbeitet. Der Fokus der Arbeit bleibt somit bewusst auf der konzeptionellen und strategischen Betrachtung der technischen Infrastruktur beschränkt.

3.Risikoanalyse

Im Rahmen einer Risikoanalyse wird die bestehende Infrastruktur der Arztpraxis systematisch bewertet. Grundlage bildet die Risikobewertung (siehe Anhang 1), in der die identifizierten Gefährdungen hinsichtlich Eintrittswahrscheinlichkeit, Schadensausmass und des daraus resultierenden Risikos beurteilt werden. Auf Basis dieser Analyse werden geeignete Gegenmassnahmen definiert und eine Handlungsempfehlung abgegeben.

4.Technische Massnahmen

4.1. WLAN deaktivieren

Für WLAN benötigt es in der Regel keinen physischen Zugriff, daher bietet es optimale Voraussetzung für Angriffe. Hier ist auch das eingesetzte Protokoll relevant, wobei in der Regel meistens veraltete, bewährte Protokolle zum Einsatz kommen. Es muss schlussendlich auch immer eine gewissen Kompatibilität gewährleistet werden.

Alle Geräte sollten deshalb ausschliesslich kabelgebunden am Netzwerk angeschlossen sein. Ein Netzwerkkabel durch einen Elektriker verlegen lassen, ist heute deutlich günstiger als noch vor 10 Jahren und daher eine sinnvolle Investition.

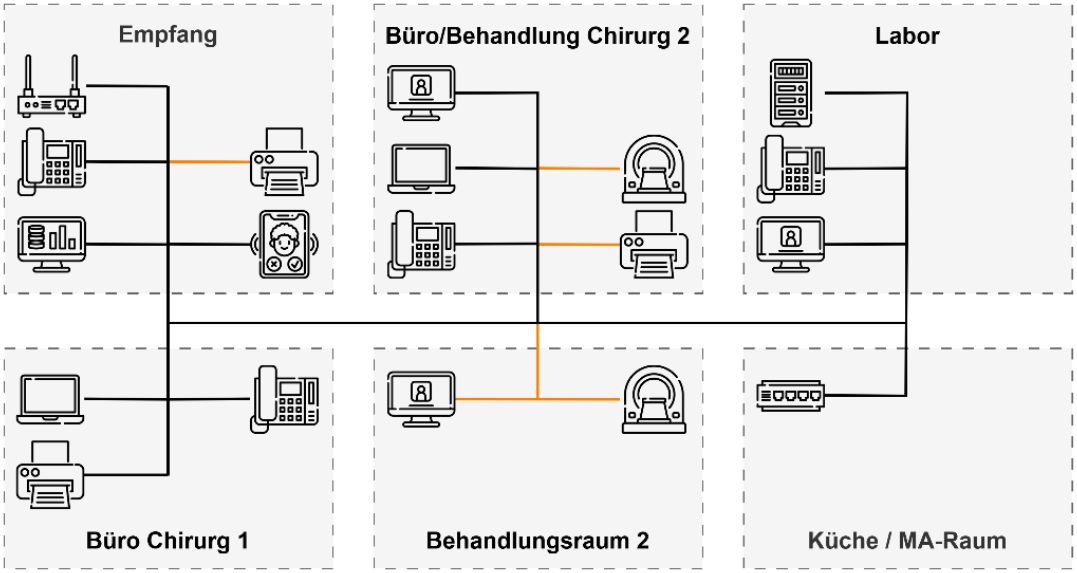

Abbildung 2: Angepasste Netzwerktopologie ohne WLAN

4.2. Mobile Endgeräte reduzieren

Die Anzahl mobiler Endgeräte (Laptops) sollte reduziert und auf ein Minimum begrenzt werden. Diese stellen im Vergleich zu stationären Arbeitsplatzrechnern ein erhöhtes Sicherheitsrisiko dar und aufgrund ihrer geringen Grösse und Transportfähigkeit können sie leichter entwendet werden. Innerhalb der Praxisräume sollte man deshalb ausschliesslich stationäre Arbeitsplätze verwenden. Laptops hingegen sind optimal für Hausbesuche oder administrative Arbeiten im Homeoffice. Zudem sind stationäre Arbeitsplätze in der Regel zuverlässiger und verringern dadurch automatisch als positiver Nebeneffekt den Supportaufwand.

Da im Auftrag keine Informationen zur eingesetzten Software oder zur Arbeitsweise der einzelnen Mitarbeiter vorliegen, wird diese Massnahme lediglich als Empfehlung abgegeben. Es kann sein, dass die Laptops in den Büros zwingend benötigt werden.

4.3. Kritische Geräte umplatzieren

Geräte wie Router und Switch gelten als kritisch und sollten nicht in frei zugänglichen Räumen platziert werden. Auch sollte der Hauptrechner nicht direkt im Empfang stehen, sondern in einem besser gesicherten Raum. Der Hauptrechner kann zum Beispiel einfach mit einem vorhandenen Client in der Praxis getauscht werden.

Aus folgenden Gründen würde sich das Labor als bester Standort auszeichnen:

- Besucher und Patienten haben dort keinen Zutritt.
- Da im Labor vermutlich weitere Geräte Geräusche verursachen, wäre die Beeinträchtigung geringer als in einem der anderen Räume.
- Der Server steht als weiteres kritisches Gerät bereits im Labor.
- Nicht alle Mitarbeiter haben Zutritt, wodurch sich im Falle eines Vorfalls die Anzahl der Personen reduzieren würde.
- Im Labor steht ein Computer, der sich möglicherweise relativ einfach durch den Hauptrechner am Empfang ersetzen liesse.

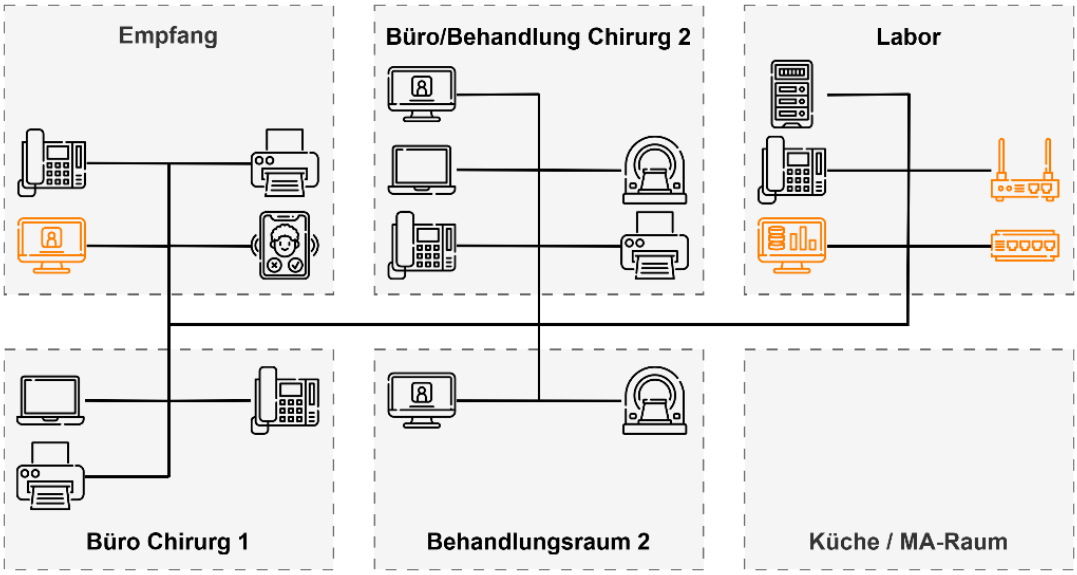

Abbildung 3: Angepasste Netzwerktopologie mit umplatzierten Geräten

4.4. MAC-basierte Zugriffskontrolle

Da es sich über eine überschaubare Anzahl Geräte handelt, könnte beispielsweise eine MAC-basierte Zugriffskontrolle eingeführt werden. So kann sichergestellt werden, dass nur die Geräte mit dem Netzwerk kommunizieren können, welche bekannt sind.

Eine MAC-basierte Authentifizierung bietet keinen absoluten Schutz gegen Angriffe, da die MAC-Adresse gespooft werden kann (Portnox, 2026), aber es bietet eine weitere Hürde und weiteren Aufwand für einen Angreifer. Heutzutage bieten fast alle modernen Netzwerkgeräte die Funktion einer MAC-basierte Filterung an. Für die Umsetzung müsste somit nur auf den Netzwerkkomponenten die MAC-Adressen erfasst werden.

4.5. Zusätzliche Datensicherung

Der Einsatz eines zusätzlichen NAS erhöht die Datensicherheit erheblich, da eine separate Datensicherung innerhalb der Praxisumgebung ermöglicht wird. Selbst wenn sich das NAS im gleichen Raum wie der Server befindet, schützt es vor typischen Risiken wie Hardwaredefekten oder Ransomware-Angriffen.

Angesichts der aktuellen Gegebenheiten sowie der erhöhten Datenschutzanforderungen im medizinischen Umfeld wird auf die Umsetzung eines Offsite-Backups vorerst verzichtet.

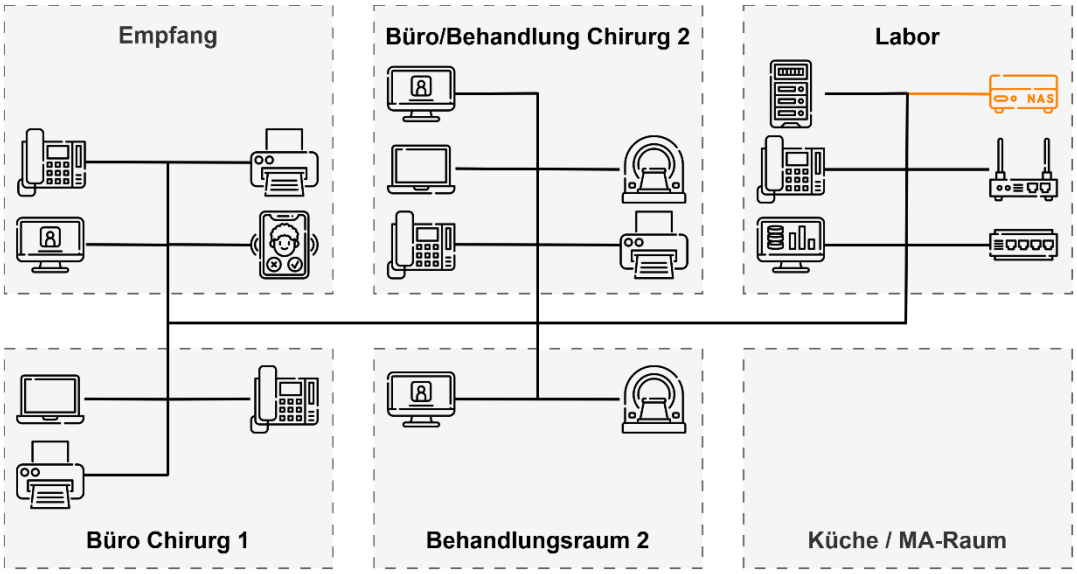

Abbildung 4: Angepasste Netzwerktopologie mit Backup

4.6. Netzwerk segmentieren

Das Netzwerk sollte in verschiedene VLANs unterteilt werden. Dadurch werden Broadcast-Domänen getrennt und der Datenverkehr effizienter gesteuert. Zusätzlich erhöht die Segmentierung die Sicherheit, da sensible Bereiche logisch voneinander isoliert werden können. Die Geräte sollten nach Funktion gruppiert werden, unabhängig von ihrer physischen Lage.

Für die Arztpraxis bietet sich folgende Aufteilung an:

VLAN ID	Name	Beschreibung
1	Management	Standard VLAN für alle Management-Geräte
10	Internal	Alle vertrauenswürdigen Geräte wie Computer, Server und NAS
20	Phone	Separates VLAN für die Telefone und den Anrufbeantworter
99	Untrusted	Für alle eher unsicheren Geräte (Drucker, Röntgengeräte, usw.)

Tabelle 1: VLAN-Übersicht

5.Handlungsempfehlung

Zur Erhöhung der Sicherheit empfiehlt es sich, die identifizierten Massnahmen gebündelt und systematisch innerhalb eines Zeitraums von etwa 3-6 Monaten umzusetzen. Die Reihenfolge der Umsetzung sollte dabei risikobasiert festgelegt werden, sodass zunächst die kritischen Schwachstellen adressiert werden.

Um einen störungsarmen Praxisbetrieb sicherzustellen, sollte die Implementierung in enger Zusammenarbeit mit einem spezialisierten IT-Dienstleister durchgeführt werden.

Die nachfolgende Grafik zeigt das gewünschte Ergebnis nach Umsetzung aller vorgeschlagenen Massnahmen:

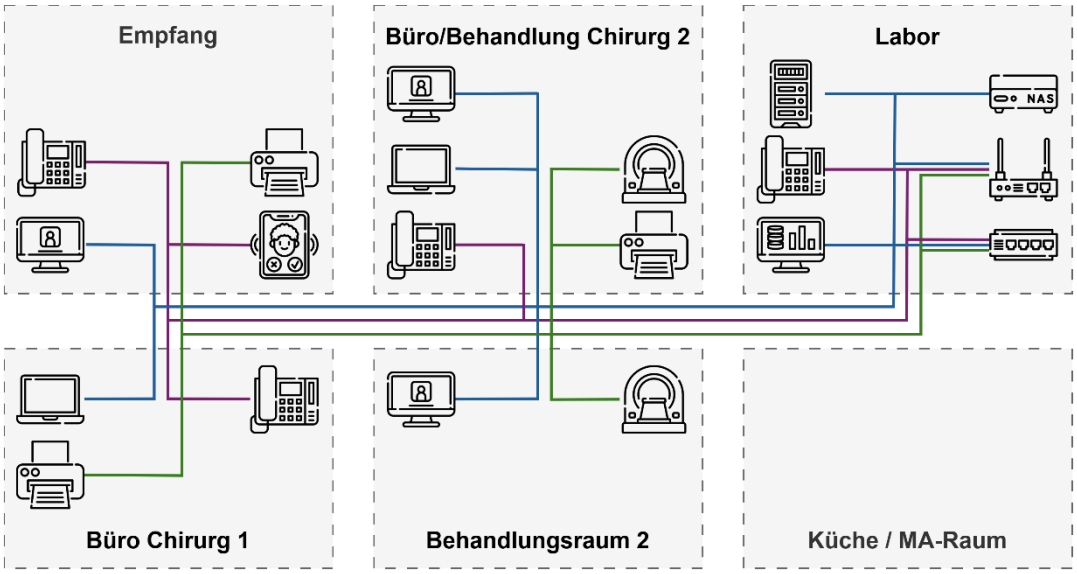

Abbildung 5: Netzwerktopologie nach der Umsetzung

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

MAC	Media Access Control
NAS	Network Attached Storage
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network

Quellenverzeichnis

Icons in den Grafiken von Freepik. (1. März 2026). Von https://flaticon.com abgerufen

Portnox. (4. März 2026). Von https://www.portnox.com/cybersecurity-101/cyber-threats/spoofing-mac-address/ abgerufen

Anhang 1: Risikobewertung

Nr.	Risiko	Eintrittswahrscheinlichkeit	Schadensausmass	Bewertung	Gegenmassnahme
1	Angriff über WLAN	Hoch	Hoch	Kritisch	Kapitel 4.1
2	Angriff über einen gepatchten Netzwerkanschluss	Mittel	Hoch	Kritisch	Kapitel 4.4 / 4.6
3	Diebstahl mobiler Geräte	Mittel	Hoch	Kritisch	Kapitel 4.2
4	Datenverlust durch Ransomware-Angriffe	Mittel	Hoch	Kritisch	Kapitel 4.5
5	Angriff über einen frei zugänglichen Computer	Niedrig	Mittel	Hoch	Kapitel 4.3
6	Angriff über einen Mitarbeiter	Niedrig	Mittel	Hoch	Kapitel 4.2 / 4.3

Tabelle 2: Risikobewertung