Checkliste Praxisrechner und Internet

Vorbemerkung:

Die Checklisten dienen zur Absicherung der Praxis-EDV vor Angriffen von innen und außen.
Der Arzt ohne fundierte Kenntnisse wird mit Ausführungen sicher überfordert sein.
Die Checklisten sollen als Prüfsteine zur Besprechung mit dem Systemtechniker der Praxis dienen. Er wird die Checklisten verstehen und muss sie umsetzen. Er sollte dem Arzt dann auch die einzelnen Maßnahmen erklären können.

Allgemein:

Die **erste Checkliste** beschreibt die Voraussetzungen, die mindestens vorliegen müssen, damit ein Rechner eines Praxisnetzes mit dem Internet verbunden werden darf.

Rechner, die diese Voraussetzungen nicht erfüllen, müssen von der Kommunikation des Praxisnetzes nach außerhalb ausgeschlossen werden. Möglichkeiten dazu werden in der **zweiten Checkliste** dargestellt. Die Kommunikation des PVS kann nur ungestört über spezielle Freigaben dargestellt werden, wenn ein Zugriff auf Dokumente von außerhalb, die über den TI-Nachrichtendienst KIM integriert wurden, NICHT aufgerufen / angezeigt werden können. Die Anzahl dieser Rechner sollte minimiert werden.

Die Sicherheitsaspekte für den Router und die Switches beschreibt die **dritte Checkliste**.

Damit der Hausarzt selbst überprüfen kann, ob die getroffenen Maßnahmen des Technikers greifen, sind in **Tabelle 4** einige einfach und vom Laien durchzuführende Tests beschrieben.

Die Checkliste ist prinzipiell produktunabhängig formuliert. Da jedoch von einer großen Verbreitung von Microsoft® Betriebssystemen ausgegangen wird, sind einige Empfehlungen jedoch Microsoft Windows® spezifisch – sollten Sie ein anderes Produkt einsetzen, so versuchen Sie bitte, entsprechende Maßnahmen einzurichten.

Glossar:

Internet-Standard:
Das Rechner-System, auf dem das HPM installiert ist und welches für die Online-Übermittlung der Daten freigeschaltet werden muss. In der Regel ist das der Server, da auch dieser in der Regel für die Installierung der Updates des PVS online angebunden sein muss. Darüber hinaus müssen alle Rechner, die mit dem Internet verbunden sind, diesem Standard genügen. Das gilt insbesondere auch für alle Rechner, die Dokumente öffnen können, die über den Nachrichtendienst KIM empfangen wurden und noch nicht einer Überprüfung auf Schadsoftware durchlaufen haben.

„alte Rechner“:
Bei einigen alten medizinischen Peripheriegeräten (EKG …) ist auf Grund deren Treiber ein Betrieb an einem Rechner mit aktuellem Betriebssystem nicht möglich. Daher müssen dort besondere Schutzmaßnahmen getroffen werden, die verhindern, dass unkontrollierte Dateien auf diesen Rechner gelangen können. Grundsätzlich muss geraten werden, diese Rechner mittelfristig auszumustern. Bis dahin sollte er möglichst isoliert sein. Der Zugriff auf das PVS muss eingeschränkt werden: wegen der Unsicherheit von über KIM eingespielten Dateien dürfen diese an diesen Rechnern NICHT geöffnet werden.

PVS:
Praxisverwaltungssystem ist die Software, die für die Dokumentation der Patientendaten erforderlich ist.

Checkliste 1

	Ziel	Maßnahme	Bedeutung	Erfolgt?
1.	**Schutzmaßnahmen für den Rechner, der mit dem Internet kommunizieren muss**	„Internetstandard“		
1.1	Unterbinden, dass wichtige Systemparameter geändert werden können	Die Sicherheitsrichtlinien sind so zu konfigurieren, dass die folgenden Einstellungen nicht durch Anwender geändert werden können: • Netzwerkeinstellungen • Windows-Registry • Installation von Programmen Die Änderung / Installation darf ausschließlich durch Konten mit administrativen Rechten erfolgen.	Muss	
1.2	Zugangsbeschränkung / Passwörter	Physisch und mittels extra Kennwort Einzigartige Passwörter (unterschiedliche Passwörter für Administrator und normalen Anwender) Starke Passwörter (ausreichende praktikable Länge je nach Anwendung insbesondere für die Administratorenrechte) ggf. Passwortmanager Keine Passwörter für Fremde auffindbar notieren	Muss	
1.3	Schnittstellenbeschränkung	USB und andere Ports beschränken (nur bekannte Peripherie/Festplatten) werden erkannt Cave: on-board Bluetooth und WLAN neuerer Rechner (AUSSCHALTEN)	Muss	

1.4	Datenträgerbeschränkung / Schutz und Entsorgung	Sicherstellen, dass nur Datenträger (bspw. USB-Sticks, DVDs) aus vertrauenswürdigen Quellen angeschlossen werden, um Datenaustausch (z.B. Betriebssystem-Updates, Applikations-Updates) vorzunehmen. Nach Möglichkeit softwaretechnische Restriktion der Nutzung von Wechseldatenträgern gegen ungewollten Datenaustausch implementieren. Verschlüsselung aller Festplatten, auf denen sich sensible Daten befinden, insbesondere in Server, Laptops, Tablets, mobile Festplatten der Datensicherung (z.B.: Bitlocker, Standartprogramm in Windows) Wiederherstellungsschlüssel separat aufbewahren (z.B. CD o.ä.) Zu entsorgende Festplatten / USB-Sticks sicher destruieren	Muss	
1.5	Firewall	• nur die erforderlichen Ports sind geöffnet • Anfragen aus dem Internet werden alle verworfen werden • keine Dienste (bspw. SSH, FTP, etc.) können im Internet angeboten werden • Nur definierte Programme dürfen auf das Internet zugreifen • Definieren einer White-List mit entsprechenden Adressen automatische Aktualisierung der Firewall und KONTROLLE !	Muss	
1.6	Virenscanner	Automatische Aktualisierung der Virenscanner und KONTROLLE !	Muss	
1.7	Betriebssystem	• Automatische Aktualisierung des Betriebssystems und aller erforderlichen Programme und KONTROLLE • Abschalten der Telemetriedaten die an den Hersteller gesendet werden	Muss	
1.8	Programme	• Deinstallieren von Programmen die nicht benötigt werden • Kritische Nutzung von Browser, E-Mail (insbesondere Anhänge) • Abschalten der Telemetriedaten die an den Hersteller gesendet werden (insbes. Office) • Makros deaktivieren (insbesondere Office-Programme) • Kontrolle ob alle installierten Programme aktuell sind?	Soll	

Checkliste 2

	Ziel	Maßnahme	Bedeutung	Erfolgt?
2.	**Verhindern des Internetzugriffs für „alte“ Rechner**	Alte Rechner sind alle Rechner, die nicht dem „Internetstand“ entsprechen		
2.1	Unterbinden, dass wichtige Systemparameter geändert werden können	Die Sicherheitsrichtlinien sind so zu konfigurieren, dass die folgenden Einstellungen nicht durch Anwender geändert werden können: • Netzwerkeinstellungen • Windows-Gruppenrichtlinien • Windows-Registry • Installation von Programmen Die Änderung / Installation darf ausschließlich durch Konten mit administrativen Rechten erfolgen.	Muss	
2.2	Zugangsbeschränkung / Passwörter	Physisch und mittels extra Kennwort Einzigartige Passwörter (unterschiedliche Passwörter für Administrator und normalen Anwender) Starke Passwörter (ausreichende praktikable Länge je nach Anwendung insbesondere für die Administratorenrechte) ggf. Passwortmanager Keine Passwörter für Fremde auffindbar notieren	Muss	
2.3	IP Bereich beschränken	• IP Adresse nur aus dem 192.168.ppp. Bereich • Keine IPv6 erlauben	Muss	
2.4	Programme	Deinstallieren von Programmen die nicht benötigt werden (insbesondere Browser, Mailprogramm, Flash- oder Mediaplayer)	Muss	

2.5	Virenscanner	Deinstallieren (hat zu viele Rechte und birgt als nicht aktuelles Tool mehr Risiken als Nutzen	Muss	
2.6	Datenträgerbeschränkung / Schutz und Entsorgung	Sicherstellen, dass nur Datenträger (bspw. USB-Sticks, DVDs) aus vertrauenswürdigen Quellen angeschlossen werden, um Datenaustausch (z.B. Betriebssystem-Updates, Applikations-Updates) vorzunehmen. Nach Möglichkeit softwaretechnische Restriktion der Nutzung von Wechseldatenträgern gegen ungewollten Datenaustausch implementieren Verschlüsselung aller Festplatten, auf denen sich sensible Daten befinden, insbesondere in Server, Laptops, Tablets, mobile Festplatten der Datensicherung (z.B.: Bitlocker, Standartprogramm in Windows) Zu entsorgende Festplatten / USB-Sticks sicher zerstören	Muss	
2.7	Updates / Installation von Peripheriegeräten	Updates von Vertragssoftware oder geprüfte Treiberdateien und Software kann auf einem freigegebenen Laufwerk des gesicherten Servers liegen und von dort bezogen werden	Soll	
2.8	KIM-Dateien	Der Zugriff auf oder das Öffnen von Dokumenten, die über den KIM Zugangsdienst oder über andere gesicherte Kanäle in das Praxisnetz integriert wurden, darf nicht möglich sein. Davor muss unbedingt eine aktive Suche nach Schadsoftware in jedem dieser Dokumente erfolgt sein.	Muss	

Checkliste 3

	Ziel	Maßnahme	Art der Umsetzung	Erfolgt?
3.	**Absicherung Router / Switch**			
3.1	Firmware	Automatische Updates der Firmware und KONTROLLE		
3.2	Hauptnetz/Gastnetz	Viele Router können so eingestellt werden, dass ein gesichertes Hauptnetz und ein Gastnetz mit dem Internet verbunden wird. Damit kann man zusätzlichen Rechnern in der Praxis den Internetzugang ermöglichen, obwohl sie keinen Zugriff auf das eigentliche Praxisnetz haben (z.B. BHÄV-TV oder ein WLAN Hotspot). Der Internetzugang für das Praxisnetz bekommt einen eigenen IP Bereich (aaa): 192.168.aaa.111, während die eigentliche Kommunikation des PVS sich auf einem anderen Bereich abspielt (192.168.ppp.123). Damit können Rechner, die nicht zusätzlich einen 2. IP Bereich (aaa) haben, nicht direkt mit dem Internet Kommunizieren. Feste IP-Adressen, kein DHCP (Zugriff für Eindringling der sein Laptop per LAN-Kabel einstöpselt wird erschwert) LAN-Steckdosen schützen, leere Steckplätze versiegeln oder vom Netz trennen WLAN für Patienten nur ohne Zugang zum Praxisnetz WLAN – Nutzung für Praxisnetz nicht empfohlen	Muss	
3.3	Zugriff auf die Verwaltungsoberfläche absichern	Der Zugriff auf die Verwaltungsoberfläche (Fat-Client / Web-Interface / Konsole) darf nur über einen besonderen passwortgeschützten Benutzer möglich sein. Der Zugriff auf die Verwaltungsoberfläche darf nur aus dem internen Netzwerk und nur mit einem sicheren Protokoll (bspw. https) möglich sein.	Muss	

Tabelle 4

	Maßnahme			
4	Absicherungsprüfung	Erwartetes Ergebnis	**Korrekt ?**	**gerügt?**
4.1	Einstecken eines USB-Sticks	Er wird nicht erkannt, es können keine Dateien gesehen werden		
4.2	Einlegen eines Datenträgers (DVD, CD o.ä.)	Er wird nicht erkannt, es können keine Dateien gesehen werden		
4.3	Suchen des Emailprogrammes	Nicht zu finden		
4.4	Suchen des Internetbrowsers	Zumindest nicht einfach zu finden		
4.5	Aufrufen einer normalen Internetseite	Zugriff verweigert		
4.6	Erstaufruf eines KIM-PDFs	Zugriff verweigert		