| In Zusammenarbeit mit dem IT-Security-Dienstleister und Systemhaus *in.sec GmbH* haben wir eine praxisnahe Checkliste erstellt, mit der wir Sie für die Gefahren hinsichtlich Sicherheit, Datenschutz und Datenintegrität beim Betrieb Ihrer IT-Anlage sensibilisieren möchten. Wenn Sie eine dieser Fragen mit ja beantworten können, besteht ein Defizit, das Ihrem Unternehmen schaden kann und auch durch Aufsichtsbehörden in Frage gestellt wird sowie mit Bußgeldern geahndet werden kann.  Die Liste erhebt keinen Anspruch auf Vollständigkeit und auch nach Korrektur dieser Fehler sind Sie nicht zwingend umfassend geschützt. Sie legen aber den Grundstein dafür, indem Sie sich der Gefahren bewusst werden ‒ und handeln.  (IT-)Sicherheit lässt sich nicht schnell herbeiführen und ist dann dauerhaft gegeben. Vielmehr handelt es sich um einen Prozess, der sich mit Ihrem Unternehmen weiterentwickeln muss.  Für eine unabhängige Hilfestellung und Beratung (bei Bedarf auch technische Umsetzung) können Sie unseren Partnerdienstleister gerne kontaktieren. Die Kontaktdaten finden Sie weiter unten. |
| --- |

|  |  |
| --- | --- |
|  | **Arbeiten Sie mit administrativen Rechten auf einem Ihrer PCs?**  Ziel von Schadsoftware ist es häufig, sich auf dem Zielsystem administrative Rechte zu verschaffen, um sich selbst dauerhaft zu installieren und sich in anderen Systemen Ihres Netzes zu verbreiten. Sie sollten daher mit Benutzerkonten ohne administrativen Zugriff arbeiten, um so den Zugriff auf Ihr System entsprechend zu erschweren. |
|  | **Nutzen Sie einen PC, den Sie als Arbeitsplatz verwenden als Server oder zentralen Speicherort Ihrer Daten?**  Häufig werden PCs an den Anmeldungstresen von Arztpraxen als Serversystem eingesetzt. Wird dieser Rechner von Schadsoftware infiziert, sind auch imminent die Daten Ihrer kompletten Praxis in Gefahr. |
|  | **Können Sie Markos in Office-Dokumenten ausführen?**  Die Microsoft Office-Produkte (Word, Excel etc.) sind prädestiniert für Angriffe, da sie in vielen Praxen vorhanden sind und die Schutzfunktionen in der Voreinstellung nicht wirksam sind. Die Funktion, Software in Dokumente einzubetten, dient hier als Infektionsweg. Das Öffnen eines per E-Mail erhaltenen Word-Dokumentes reicht bereits für die Infektion. Die vorgesehene Sicherheitswarnung wird von Mitarbeitern meist ignoriert und bietet keinen Schutz ‒ Ziel des Mitarbeiters ist es schließlich, an den Inhalt des Dokuments zu gelangen. Auch können diese Dokumente von bekannten Empfängern stammen, die ihrerseits wiederum bereits mit Schadsoftware infiziert sind, ohne dies zu bemerken. Deaktivieren Sie daher grundsätzlich die Makrofunktion in Office-Dateien. |

|  |  |
| --- | --- |
|  | **Sie führen keine regelmäßige vollständige Wiederherstellung und Funktionstests Ihrer Backups durch?**  Das Wiederherstellen eines Backups in regelmäßigen Abständen und der anschließende Funktionstest der Inhalte ist eine Grundvoraussetzung eines Back­up-Konzeptes. Woher wissen Sie sonst, ob Ihr Backup funktioniert? Ohne diese Maßnahme können Sie nicht ausschließen, dass Sie über lange Zeit Sicherungen durchführen, die im Krisenfall nutzlos, weil dysfunktional sind. |
|  | **Lagern Sie Ihr Backup in den Praxis-/Klinikräumen?**  Die Sicherung Ihrer Daten auf Datenträgern oder in Netzwerkspeichern, die sich in den gleichen Räumlichkeiten wie Ihr Serversystem befindet, ist nicht gegen elementare Gefährdungen geschützt. Bei Feuer, Wasser, Beschädigung, Einbruch, Diebstahl, Sabotage etc. werden beide Systeme zerstört und Sie haben keine Möglichkeit, Ihre Daten wiederherzustellen. |
|  | **Nutzen Sie für Ihren Heimarbeitsplatz Teamviewer, Anydesk oder einer andere Fernwartungslösung?**  Die Zweckentfremdung von Fernwartungslösungen exponiert die Daten potentiell dem Hersteller der Lösung. Zudem bietet ihre Nutzung eine Angriffsfläche auf Ihrem System. Für Heimzugänge müssen daher zu diesem Zweck vorgesehene VPN-Lösungen eingesetzt werden, bei denen die Daten zweifelsfrei direkt und ohne Mittelsmann zu Ihrer Praxis übertragen werden. |
|  | **Halten sich Patienten oder andere fremde Personen (auch nur kurz) unbeobachtet an Orten in Ihrer Praxis/Klinik auf, an denen sie auf PCs, Netzwerkanschlüsse oder sensible Informationen zugreifen können?**  Patienten, die in einem Raum allein sind, haben ohne weiteres die Möglichkeit, technische Geräte für spätere Angriffe an Ihr IT-System anzuschließen. Dieser Angriffsweg muss mit technischen und organisatorischen Maßnahmen unterbunden werden. Auch das beobachtete Eintippen Ihrer Passwörter oder der Blick des Patienten auf die Struktur Ihres IT-Systems verrät viele Informationen, die Angriffspotential bieten. |
|  | **Haben Sie Ihren Mitarbeitern die Privatnutzung der IT-Systeme schriftlich untersagt?**  Falls nicht, werden sie die IT auch privat nutzen. Das erhöht die Gefahr, Schadsoftware einzubringen oder sensible Informationen versehentlich im Internet zu exponieren. |
|  | **Ihr Telematik-Konnektor hängt immer wieder und die Kollegin hat sich schon darum gekümmert, dass das Systemhaus das endlich löst?**  *"Hallo Hier ist ... von <Hersteller Ihres AIS-Systems>! Ich hab ja mit Ihrer Kollegin vor einigen Tagen wegen dem Update für Ihren Konnektor gesprochen, weil der immer wieder hing und Sie neustarten mussten. Ich hätte jetzt vor meinem Meeting noch ein paar Minuten Zeit, dass wir zusammen das Update installieren! Ja? Dann starten Sie mir bitte mal den Teamviewer und geben Sie mir Ihre ID …"*  Social Engineering Angriffe, der Enkeltrick der IT-Security-Szene, gehören mittlerweile zum Tagesgeschehen. Sie wären überrascht, wie viele Mitarbeiter wir unter Realbedingungen dazu bringen, eine Fernwartungssitzung zu öffnen. Und ja, sogar die Nummer im Display Ihres Telefons kann mit einer relativ einfachen Simulation wie die Ihres Systemhauses wirken. Daher sollten Sie Routinen festlegen, wie Sie sicherstellen können, dass Sie auch mit den richtigen Personen sprechen und keinem Betrüger aufsitzen. |

Sollten Sie Fragen haben oder eine Beratung wünschen, steht Ihnen unser Partner selbstverständlich gerne zur Verfügung:

|  |  |
| --- | --- |
|  | **in.sec GmbH** www.insec.gmbh  Kontakt: Simon Harlacher <sh@insec.gmbh> (+49-176-60971019) |