Immer häufiger sind kleine und mittelständische Unternehmen bis 250 Mitarbeiter, wie Kliniken, MVZ´s und Arztpraxen, das Ziel von Hackern. Hier ist man laut dem aktuellen Intelligence Report von Symantec am schlechtesten geschützt. Gegenüber 2011 hat sich die Zahl der gezielten Angriffe dort verdoppelt. Etwa ein Drittel aller Angriffe galt alleine diese „Zielgruppe“. Hinzu kommen die latenten Gefahren durch Viren und Trojanern, der alle ausgesetzt sind und welche inzwischen auch auf gesicherten Wegen, wie Intranetverbindungen oder KV-Safenet, immer häufiger Ihr Ziel finden.

Grundsätzlich gibt es hierfür zwei Hauptursachen:

Viele verantwortliche Inhaber dieser Praxen und Unternehmen unterschätzen die Bedrohungssituation, da es ja bei Ihnen nach eigenen Einschätzung nichts Wertvolles zu holen gibt. Doch auch mit scheinbar unwichtigen Daten wie Patienten- oder Kundendaten und den damit in Verbindung stehenden Informationen und Dokumentationen, ist heute leicht viel zu verdienen.

Zum anderen ist fehlendes Know-how oder nicht ausreichend geschulte (oder interessierten) Mitarbeiter/innen oft die Ursache für abgelaufenen Virenschutz oder fehlende System- und Sicherheitsupdates.

Hinzu kommt dann noch die leider oft falsche Einschätzung der verantwortlichen beim Kosten-Nutzenvergleich für eine professionelle Schutzlösung. „*Bei uns ist noch nie etwas passiert* “ hören wir dann oft. Doch eine Analyse der vorgefundenen Anlage zeigt im Audit dann meist mehr als nur die bekannten trackingcookies. In über **75% der von uns untersuchten Anlagen, finden wir Trojaner oder Viren** vor, welche bereits direkt oder indirekt Schäden verursacht haben. Was die Aussage der verantwortlichen wie „ *Bisher ist doch alles gut gegangen* “ eindeutig widerlegt.

Dabei sind es häufig nur kleine Veränderungen am System oder eine Schulung der Mitarbeiter/innen welche so etwas verhindern, und die Netzwerksicherheit erheblich steigern können.

Auch heute kann man noch guten Gewissens „online“ gehen und die Praxisabläufe unter Einbindung von Internet und e-Mail optimieren. Dies bitte aber auf der Grundlage einer sicheren Anbindung und unter Berücksichtigung der individuellen Bedürfnisse.

Nur ein Beispiel: Sie haben nicht volljährige Auszubildende oder Praktikanten und diese haben Zugang zu einem Arbeitsplatz mit Internet? Dann ist auf diesem Rechner sicher auch eine Jugendschutzsoftware installiert. Denn sonst machen Sie sich als Verantwortlichen Inhaber oder Ausbilder strafbar, da sie den Jugendlichen ja z.B. pornografisches Material zugänglich machen!

In allen Fragen um Ihre IT steht Ihnen unser Team gerne zur Verfügung. Sprechen Sie uns an!

Unter dem Motto Die Praxis im Internet mit Sicherheit ja!