Wenn sich **ein Virus** als Bewerbung tarnt

Nur ein falscher Klick, und alle Daten sind verschlüsselt. Nicht nur in Arztpraxen häuften sich zuletzt die Schadenfälle, bei denen Viren als Bewerbung getarnt den kompletten **PC lahmlegten**. Die HÄVG gibt Tipps, wie Sie vorbeugen können.

Auch Hausarztpraxen können Opfer von Computerviren werden! Hier können zum Beispiel Trojaner zum Einsatz kommen, die Daten des Praxis-PC verschlüsseln und diese für die Praxismitarbeiter unzugänglich machen. Kriminelle Computerexperten könnten dann einen Geldbetrag fordern, um die Daten für die Praxis wieder freizuschalten. Die HÄVG empfiehlt folgendes Vorgehen, um sich vor Schadsoftware zu schützen: Grundsätzlich gilt auch bei der Praxis-EDV: Es gibt viele vorbeugende Maßnahmen, um einem Angriff von Schadsoftware nicht hilflos ausgeliefert zu sein.

Datensicherung

Die Daten der Praxis-EDV müssen regelmäßig, am besten täglich, gesichert werden. Datensicherung bedeutet, dass eine oder mehrere Kopien gespeicherter Daten auf einem externen Speicher erzeugt werden. So kann der Datenbestand bei einem Verlust der Daten schnell wiederhergestellt werden. Hier gilt es zwischen interner und externer Datensicherung zu unterscheiden. Diese Verfahren sind jedoch nicht ersetzend, vielmehr sollten für eine valide Datensicherung beide Verfahren parallel zum Einsatz kommen, um das Ausmaß des Schadens bei einem möglichen Angriff auf die Praxis-EDV möglichst gering zu halten.

Externe Datensicherung

Im besten Fall sollte täglich eine Datensicherung auf einem separaten Datenspeicher (zum Beispiel wechselnde externe Festplatten oder Bandlaufwerke) erfolgen. Das minimiert den Datenverlust, wenn Malware die Praxis-EDV befällt. Das Speichermedium sollte man am besten gut gesichert (Tresor o.ä.) außerhalb der Praxis aufbewahren.
Wichtig ist, in jedem Fall mehrere externe Medien für ein „rollierendes" Backup zu verwenden, so dass das gleiche Medium nicht zwei Tage hintereinander verwendet wird.
Gegen unbemerkt im Hintergrund agierende Trojaner kann etwa eine einmalige Sicherung im Quartal auf ein permanentes Medium erfolgen oder ein Speichermedium dauerhaft archiviert und durch ein Neues ersetzt werden.

Interne Datensicherung

Zusätzlich zu externen Backups, welche man hauptsächlich vor Trojanerbefall, Diebstahl oder Elementarschäden schützen sollte, ist es darüber hinaus empfehlenswert, mit internen Backups im Softwarefehlerfall schnell wieder für ein funktionsfähiges System sorgen zu können. Dazu kann eine tägliche Sicherung auf eine weitere interne Festplatte für eine schnelle Wiederherstellung der Datenbanken des Praxis-Verwaltungs-Systems (PVS) nützlich sein. Für Details einer solchen Backup-Strategie und weitere Empfehlungen wenden Sie sich bitte an Ihr Systemhaus.

Sonstige präventive Maßnahmen

Die Praxis-EDV sollte stets auf einem aktuellen Stand gehalten werden, das heißt Software-, Programm- oder sonstige EDV-Updates sollten zeitnah erfolgen. Auch ein hochwertiges und zuverlässiges Anti-Virenprogramm sollte Teil einer Abwehrstrategie sein.
Links oder Anhänge aus E-Mails von zweifelhaften Absendern sollten keinesfalls angeklickt, sondern sofort gelöscht werden. Achtung: Oft tarnen sich diese E-Mails als vermeintliche Bewerbungen!

Im Schadensfall

Auf erpresserische Geldforderungen sollten Sie keinesfalls eingehen. Es gibt keine Garantie, dass die Daten wieder freigeschaltet werden. Kriminellen kann ausgerechnet in dieser Frage nicht vertraut werden.
Das Systemhaus, die regionale KV sowie – eine HZV-Vertragsteilnahme vorausgesetzt – der Kundenservice der HÄVG Rechenzentrum GmbH sollten umgehend informiert werden.

LINK

Unsere IT-Serie verrät weitere Tricks rund um den Schutz der Praxisdaten: **http://hausarzt.link/AInZb**

Foto: Erwin Wodicka - Gina Sanders - Fotolia