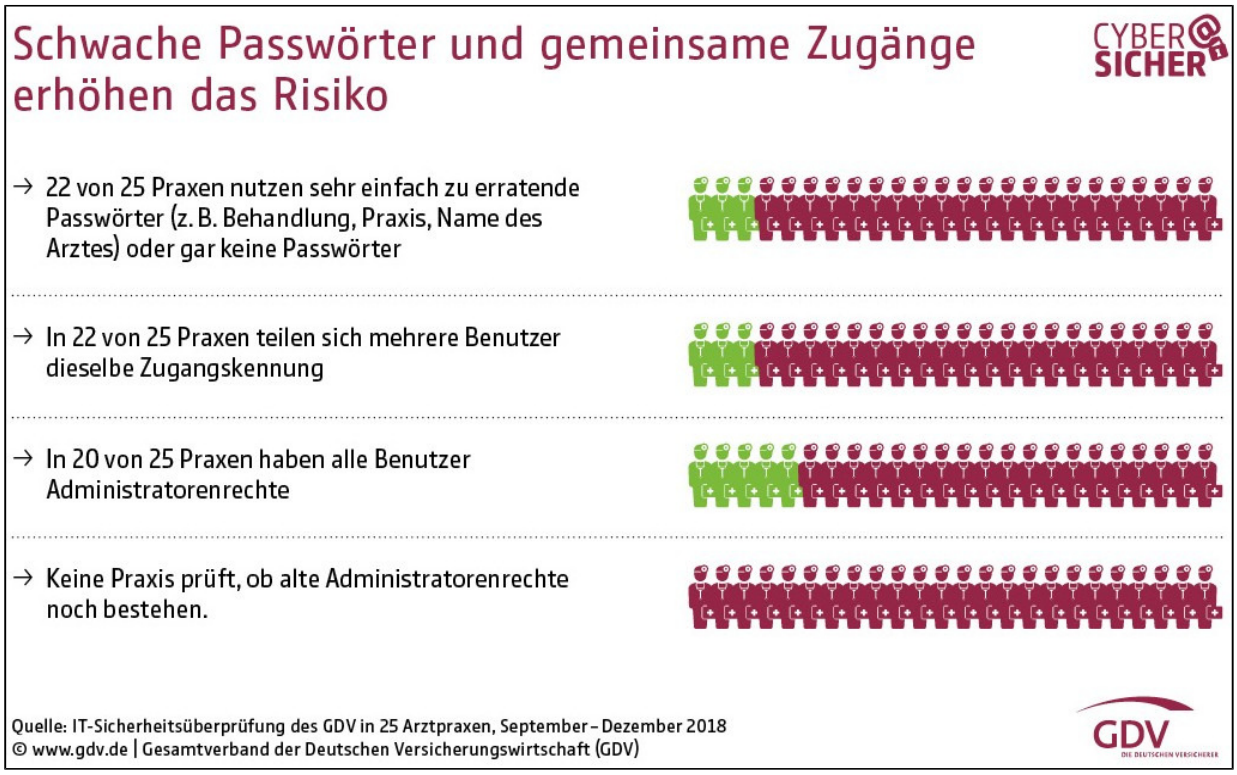
Hacker knacken spielend Passwörter in Arztpraxen

Deutschlands Ärzte gehen zu nachlässig mit Passwörtern in ihren Praxen um. Damit gefährden sie auch die Sicherheit sensibler Patientendaten. Vor allem E-Mail- und Passwort-Kombinationen – auch von Kliniken - finden sich häufig sogar im Darknet, zeigt eine Untersuchung zur IT-Sicherheit im Auftrag des GDV.

Obwohl Ärzte ihre eigenen IT-Systeme für sicher halten, zeigt die Realität ein anderes Bild. Neben einem Sicherheitscheck vor Ort hat der GDV Gesamtverband der Deutschen Versicherungswirtschaft (www.gdv.de) mit dem vollautomatisierten Analyse-Tool Cysmo die Sicherheit der IT-Systeme von 1.200 niedergelassenen Ärzten verschiedener Fachrichtungen sowie von jeweils rund 250 Apotheken und Kliniken getestet. Ein Test der Mailserver ergab, dass von den knapp 1.200 untersuchten Ärzten nur fünf (0,4 Prozent) hinsichtlich der unterstützten Verschlüsselungsmethoden auf dem vom BSI Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de) empfohlenen Stand der Technik seien. Dazu erschien auch ein neuer Branchereport **„Cyberrisiken beim Ärzten und Apotheken“**.



Demnach verwenden unter anderem neun von zehn Ärzten leicht zu erratende Passwörter wie „Praxis“, „Behandlung“ oder ihren eigenen Namen (**siehe GDV-Grafik**). In 22 von 25 freiwillig untersuchten Praxen teilen sich zudem mehrere Benutzer dieselbe Zugangskennung und haben meist auch vollständige Administratorenrechte. Dies stellt nach Meinung von Experten ein hohes Risiko dar.

81 Prozent der Ärzte sehen Computersysteme umfassend geschützt

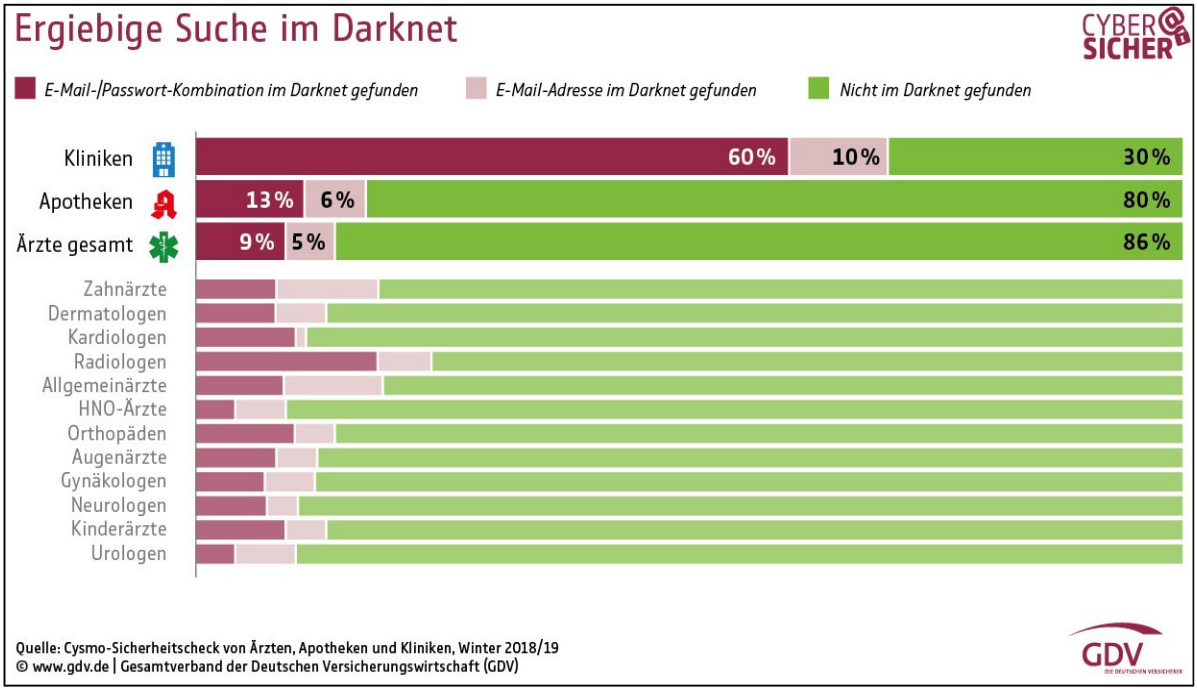
Schon zuvor wurden Ärzte und Apotheker in einer repräsentativen Forsa-Umfrage (www.forsa.de) zu ihren Einschätzungen und Erfahrungen mit der Digitalisierung und Cyberrisiken befragt. Dabei wurde das allgemeine Risiko für Arztpraxen und Apotheken von 44 Prozent als hoch eingeschätzt, das eigene mit nur 17 Prozent jedoch als eher gering. Insgesamt glauben 81 Prozent der Ärzte, ihre Computersysteme seinen umfassend geschützt. Dem Großteil sind die Folgen einer Cyberattacke bewusst. 78 Prozent der Befragten müssten nach eigener Ansicht ihre Arbeit einstellen oder stark einschränken, wenn die Praxis-IT lahmgelegt würde.

Besonders wichtig in Praxen und Kliniken sei die Mitarbeitersensibilisierung, erklärte Gert Baumeister, Vorsitzender der Projektgruppe Cyberversicherung im GDV während eines Pressegesprächs. Er präentierte beispielsweise auch eine Grafik mit Darknet-Ergebnissen (**siehe GDV-Grafik**). In einem Test mit einer fingierten Mail wurden immerhin 6 von 25 attackierten Arztpraxen Opfer des Phishing-Angriffs. Hier klickten die Mitarbeiter auf den in der Mail enthaltenen Link und luden das anhängende Word-Dokument runter. Wegen der hohen

Beschäftigtenzahl bestünde vor allem bei Kliniken ein großer Handlungsbedarf.

Gert Baumeister berichtete, dass in 9 von 25 Praxen aktuelle Sicherheitsupdates der IT-Systeme fehlten. In Kliniken mit eigenen IT-Abteilungen sieht es demnach aber deutlich besser aus. Backups zur Datensicherung werden in Praxen zwar oft durchgeführt, aber nur selten verschlüsselt und fast nie wird getestet, ob sich die Daten tatsächlich wiederherstellen lassen. Auch existiert nur sehr selten ein Notfallkonzept für das Verhalten nach einem Cyberangriff. Schließlich sind demnach viele Praxen leichte Beute bei Phishing-Attacken: In jeder zweiten Praxis öffneten Mitarbeiter eine potenziell schadhafte Mail, 20 Prozent klickten sogar auf einen Link oder öffneten den Anhang.

Gert Baumeister



Erst sichern, dann versichern

Das Vertrauen in den jeweiligen externen IT-Dienstleister ist demnach sehr hoch. Eine Besserung der Situation könnte es laut **Michael Wiesner**, Hacker und Mitglied im Chaos Computer Club (www.ccc.de), nur geben, wenn die Anbieter von IT-Dienstleistungen stärker in Haftung genommen werden könnten.

Ein Problem seien jedoch die hohen Kosten für Sicherungssysteme. Zudem sähen sich die Ärzte schon mit früheren Digitalisierungsvorschriften wie der elektronischen Patientenakte gegängelt.

Grundsätzlich könne die Dienstleistung des IT-Unternehmens durch eine Cyberversicherung ergänzt werden, hieß es in dem Gespräch mit Journalisten. Die Mindestsicherung des eigenen Systems durch ein Virenprogramm sei hierfür aber die Voraussetzung. „Erst sichern, dann versichern“, sei das Motto, sagte GDV-Experte Baumeister. (Gerald Herde / Text + Fotos / www.bocquel-news.de)