Gesamtverband der Deutschen Versicherungswirtschaft e. V.

CYBER SICHER

Eine Initiative der Deutschen Versicherer.

Branchenreport

Cyberrisiken bei Ärzten und Apotheken

GDV
DIE DEUTSCHEN VERSICHERER

Cyberrisiken bei Ärzten und Apotheken – unterschätzte Gefahr?

78 % der Arztpraxen und 97 % der Apotheken wären ohne funktionierende IT-Systeme deutlich eingeschränkt → Seite 5

Jeder zweite Arzt und Apotheker denkt, seine Praxis/Apotheke wäre zu klein, um in den Fokus von Cyberkriminellen zu geraten → Seite 5

80 % meinen, sie wären ausreichend gegen Cyberkriminalität geschützt → Seite 6

Ein Drittel der Ärzte und Apotheker plant keine weiteren Investitionen in die IT-Sicherheit → Seite 6

„Ärzte sind eine **gut erpressbare Berufsgruppe**“, sagt IT-Experte und White-Hat-Hacker Michael Wiesner → Seite 10–12

In 22 von 25 getesteten Arztpraxen nutzen mehrere Benutzer dieselbe Zugangskennung mit sehr einfachen oder gar keinen Passwörtern → Seite 13

10 von 25 getesteten Arztpraxen sind auf einen Ausfall der IT-Systeme nicht vorbereitet → Seite 15

So gut wie keine Praxis oder Apotheke ist bei der Mail-Verschlüsselung auf dem neuesten Stand der Technik → Seite 16

Kostbare Beute Patientendaten

Kaum ein Wirtschaftssektor hantiert mit so sensiblen Informationen wie das Gesundheitswesen. Mit der fortschreitenden Digitalisierung wächst der Druck auf Ärzte, Apotheken und Kliniken, die Daten ausreichend vor Hackerangriffen zu schützen.

Wer Lokalzeitungen durchkämmt, stößt auf eine Vielzahl von Cyberattacken auf Apotheken und Arztpraxen. Immer wieder geraten Betroffene in die Schlagzeilen, weil sie nach einem Angriff ihre Apotheke oder Praxis zeitweise schließen mussten: im rheinischen Kevelaer ebenso wie in Bonn, in Herbolzheim im Breisgau oder in Wolfsburg. Die Attacken zeigen, welche Folgen ein Ausfall der IT-Systeme haben kann: Im schlimmsten Fall geht gar nichts mehr.

Kein Wunder. Denn auch die Medizin setzt – Stichwort Telematik-Infrastruktur – auf die Chancen der Digitalisierung. In einer repräsentativen Forsa-Umfrage im Auftrag des GDV sagt eine knappe Mehrheit der befragten Ärzte und Apotheker auch, dass die Vorteile dieser Entwicklung überwiegen: Die Abrechnung mit Krankenkassen wird bequemer und schneller, der fachliche Austausch mit anderen Ärzten und mit Patienten wird einfacher, der Verwaltungsaufwand geringer. Soweit die Hoffnungen. Doch die Befragten sehen auch die Nachteile: Sie fürchten unter anderem hohe Kosten, Probleme bei der Übertragung bisher analoger Daten in digitale Formate und Datenschutzprobleme. Einig sind sich die Ärzte und Apotheker aber vor allem darin, dass die Bedrohung durch Cyberkriminelle im Zuge der Digitalisierung steigt.

88 % sehen in dem gestiegenen Risiko von Cyberkriminalität einen Nachteil der Digitalisierung

Die Gefahr ist also erkannt – aber gebannt ist sie allein dadurch noch lange nicht. Denn die Forsa-Umfrage und Sicherheits-Tests des GDV unter Ärzten und Apotheken zeigen auch, dass das individuelle Risiko von vielen fahrlässig unterschätzt und die Qualität der IT-Sicherheit systematisch überschätzt wird.

Wie verletzlich das Gesundheitswesen schon heute geworden ist, realisieren viele Akteure offenbar erst langsam. Dabei ist der Diebstahl von Patientendaten der Super-Gau: Sie gehören zu den sensibelsten Daten überhaupt, nicht umsonst stuft sie der Gesetzgeber als besonders schützenswert ein. Das Strafgesetzbuch sieht sogar Freiheitsstrafen vor, wenn vertrauliche Angaben von Patienten ohne deren Einwilligung öffentlich gemacht werden. Gerade deshalb bräuchten Ärzte, Apotheken und Kliniken besonders sichere Computersysteme. ←

Über die Initiative CyberSicher

Mit der Initiative CyberSicher sensibilisieren die Versicherer für die Gefahren aus dem Cyberspace und zeigen, wie sich kleine und mittlere Unternehmen schützen können. Dabei nimmt die Initiative auch die Cyberrisiken einzelner Branchen unter die Lupe.

CYBER SICHER

Eine Initiative der Deutschen Versicherer.

Fragen Sie Ihren Arzt oder Apotheker: Hackerangriffe würden Praxen lahmlegen

Den meisten niedergelassenen Ärzten und Apothekern ist bewusst, wie sehr ihre Arbeit mittlerweile von funktionierenden Computersystemen abhängig ist. Doch das Risiko, selbst einmal Opfer eines Cyberangriffs zu werden, verdrängen viele – es trifft ja immer nur die anderen.

Befällt Arztpraxen oder Apotheken ein Computer-Virus, bleiben Viren bei Patienten unbehandelt. Acht von zehn Arztpraxen und so gut wie jede Apotheke in Deutschland müssten ihre Arbeit nach einem erfolgreichen Cyberangriff einstellen oder stark einschränken. Das geht aus einer repräsentativen Forsa-Befragung im Auftrag des GDV hervor. So wären bei einem mehrtägigen Ausfall der IT nach eigenen Angaben 78 Prozent der Praxen und sogar 97 Prozent der Apotheken sehr stark oder eher stark eingeschränkt. Nur jede achte Praxis könnte bei einem mehrtägigen IT-Ausfall wenig oder gar nicht eingeschränkt weiterarbeiten. Neun Prozent der Ärzte sehen sich ein wenig, aber nicht so stark eingeschränkt. Bei den Apothekern glaubt nur jeder Hundertste, er könne bei einem Ausfall ohne Einschränkungen einfach weiter arbeiten.

Terminverwaltung, digitale Patientenakten, Bestellsoftware oder Inventarlisten: Dem starken Bewusstsein der Ärzte- und Apothekerschaft, vom Funktionieren der Technik abhängig zu sein, steht nur eine geringe Sorge gegenüber, selbst Opfer von Cyberkriminalität zu werden. Nicht mal ein Viertel der Ärzte hält das eigene Risiko, Opfer eines Hackerangriffs zu werden, für eher bzw. sehr hoch. Unter Apothekern ist das Problembewusstsein mit 17 Prozent noch weniger ausgeprägt. Die große Mehrheit sieht eine eher oder sehr geringe Gefahr, dass Hacker bei Ihnen zuschlagen. Die konkrete Gefahr, selbst Opfer eines Angriffs werden zu können, wird von deutschen Apothekern und Ärzten verdrängt.

Mich trifft es nicht, schon eher den Kollegen: Dies gilt vielen Ärzten als recht wahrscheinlich. 48 Prozent der Apotheker und 44 Prozent der Ärzte glauben, dass allgemeine Risiko von Praxen und Apotheken, Opfer eines Cyberangriffs zu werden, sei eher bzw. sehr hoch. Blicken Ärzte nicht auf die eigene Praxis, schätzen sie das Risiko eines Angriffs also gleich ganz anders ein. Eigen- und Fremdwahrnehmung klaffen beim Thema IT-Sicherheit und Hackerangriffe stark auseinander.

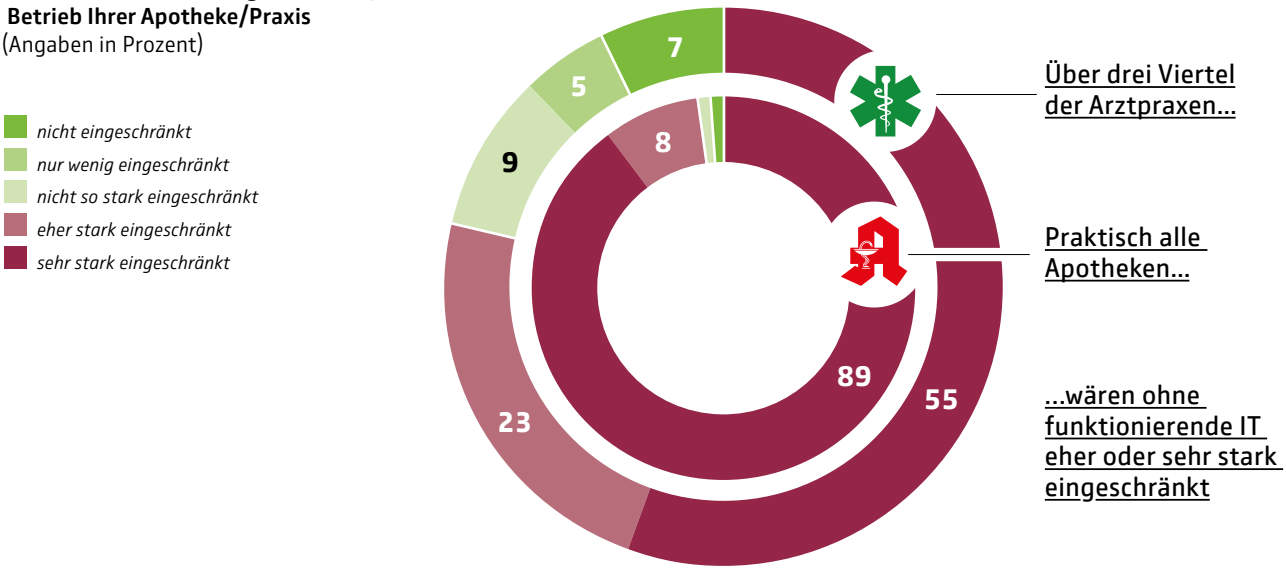
Ein Grund für den Glauben, dass es doch eher die anderen treffen werde: Vier von fünf Ärzten und Apothekern sehen sich gegen Cyberkriminalität gut gewappnet. Zum einen glauben fast alle Ärzte und Apotheker, ihre Computersysteme umfassend geschützt zu haben. Zum anderen wiegen sich viele in falscher Sicherheit, gar nicht zum möglichen Opferkreis zu gehören: Die eigenen Daten sind nicht interessant genug, die eigene Praxis ist nicht groß genug, um in den Fokus von Hackern zu kommen – diese gängigen Irrglauben sind →

Über die Umfrage „Cyberrisiken im Gesundheitswesen“

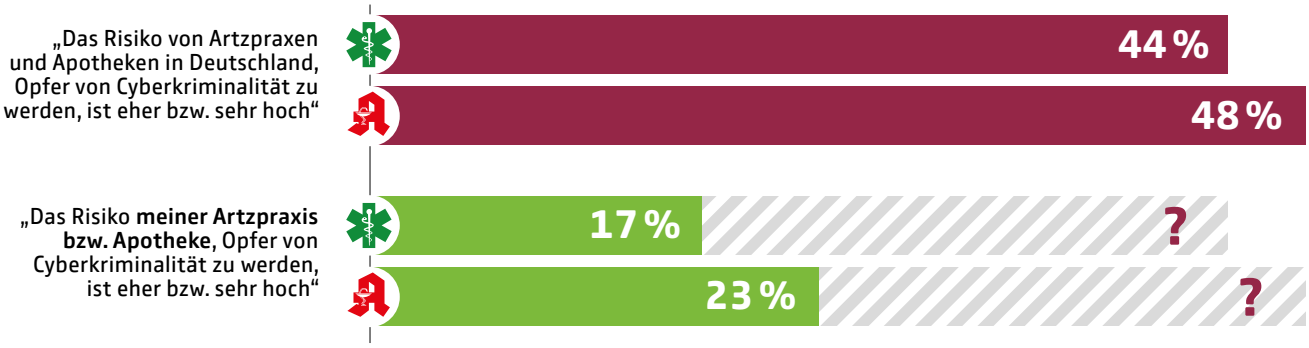
Der GDV hat die Forsa Gesellschaft für Sozialforschung und statistische Analysen mbH mit einer repräsentativen Befragung der für die Internetsicherheit zuständigen Mitarbeiter von 200 Arztpraxen und 100 Apotheken beauftragt. Die Interviews fanden zwischen dem 11. Juni und dem 6. Juli 2018 statt.

Nicht funktionierende IT-Systeme legen schnell auch die meisten Apotheken und Arztpraxen lahm

Würde die IT mehrere Tage ausfallen, wäre der Betrieb Ihrer Apotheke/Praxis
(Angaben in Prozent)



„Das Risiko gibt es – aber meine Praxis/Apotheke betrifft es nicht“



Gefährlicher Irrglaube

Obwohl Arztpraxen und Apotheken mit sensiblen Patientendaten umgehen, wiegen sie sich in Sicherheit. Von den Arztpraxen/Apotheken, die nur ein geringes Risiko sehen, sagen ...

80 %
89 %
Unsere Computersysteme sind umfassend geschützt

56 %
49 %
Meine Praxis/Apotheke ist zu klein, um in den Fokus der Cyberkriminellen zu geraten

45 %
37 %
Unsere Daten sind nicht interessant für Cyberkriminelle

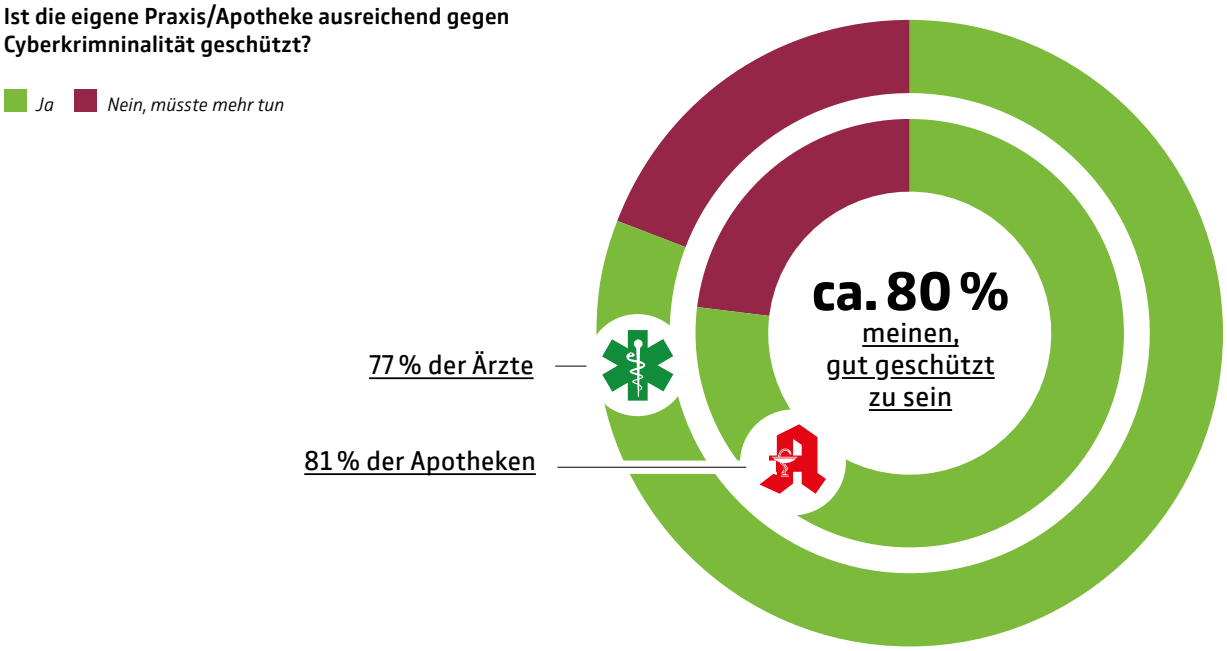
→ bei Medizinern und Pharmazeuten weit verbreitet. Rund jeder Zweite glaubt, die eigene Praxis oder Apotheke sei zu klein für Hacker.

Dabei ist mit sogenannten Ransomware-Angriffen in den vergangenen Jahren eine Spielart der Cyberangriffe populär geworden, die es Hackern ermöglicht, mit Angriffswellen lukrativ massenhaft Kleinbeträge zu erpressen – zum großen Schaden der vielen Betroffenen. Auch die Hausarztpraxis und die kleine Apotheke an der Ecke sind somit Ziele globaler Hackerbanden geworden, zumal kleine Betriebe weniger geschützt sind als große.

Zumindest für die Zukunft steht die IT-Sicherheit bei den meisten Apothekern und Ärzten auf dem Zettel: Jeder vierte Apotheker und jeder fünfte Arzt will auf jeden Fall in den kommenden zwei Jahren in IT-Sicherheit investieren. Für jeweils 36 Prozent der Ärzte ist eine Investition zumindest wahrscheinlich. Doch jeweils jeder dritte niedergelassene Mediziner und Pharmazeut wird bestimmt nicht oder eher nicht in weitere Schutzmaßnahmen gegen Cyberkriminalität investieren. Denn der Irrglaube lebt weiter: Mich selbst wird es ja schon nicht treffen. ←

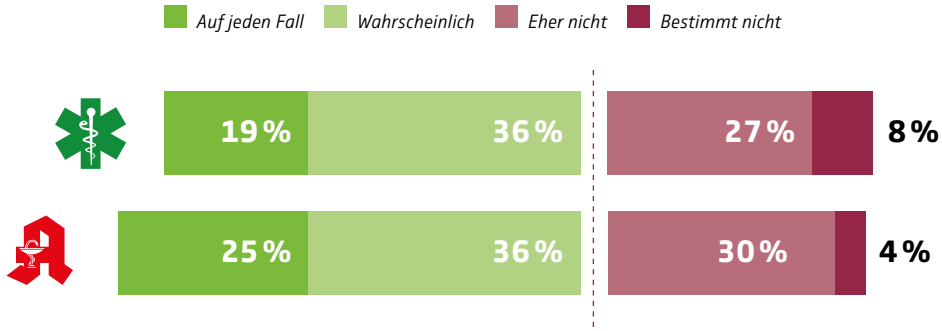
Hohes Vertrauen in den eigenen Schutz …

Ist die eigene Praxis/Apotheke ausreichend gegen Cyberkrimninalität geschützt?



… führt zu geringer Investitionsbereitschaft

Wollen Sie in den kommenden zwei Jahren in weitere Schutzmaßnahmen gegen Cyberkriminalität investieren?
An 100 % fehlende Angaben: „weiß nicht".



Was eine Cyberattacke kosten kann – und eine Cyberversicherung deckt (✓)

Musterszenario Datenklau:

Hacker attackieren die IT-Systeme einer Arztpraxis. Sie kopieren die Patientendaten und versprechen, gegen die Zahlung von Lösegeld auf eine Veröffentlichung der Daten zu verzichten.

Angriff

Die Arztpraxis erhält per Mail einen Erpresserbrief. Die Kriminellen behaupten, im Besitz aller Patientendaten zu sein. Als Beleg senden sie kompromittierende Daten über fünf Patienten, die tatsächlich in der betroffenen Praxis in Behandlung waren. Sie drohen damit, die Daten zu veröffentlichen, wenn der Arzt nicht bereit ist, ein hohes Lösegeld zu zahlen.

Informationen an Patienten und Behörden

Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt der Arzt kein Lösegeld. Er muss aber die Datenschutzbehörden und seine Patienten über den Verlust der sensiblen Daten informieren. Um sicher zu gehen, dass er seinen Pflichten in vollem Umfang nachkommt, holt er sich Hilfe bei einem Rechtsanwalt. Die Patienten sind nach der Information verunsichert und haben intensiven Gesprächsbedarf.

- *Informationskosten: 4.000 Euro*
- *Anwaltskosten: 2.000 Euro*

Security-Initiative

IT-Spezialisten suchen und schließen die Schwachstelle, die den Tätern Zugriff zu den Daten erlaubte. Die Systeme werden desinfiziert und gehärtet.

- *Kosten für IT-Forensik: 5.000 Euro*

Betriebsunterbrechung

Bis die Schwachstellen geschlossen und weitere Datendiebstähle verhindert sind, bleibt die Arztpraxis geschlossen. Auch die Abrechnung mit den Krankenkassen ist unmöglich.

- *Kosten für 2 Tage Betriebsunterbrechung: 5.000 Euro*

Datenmissbrauch

Die Hacker veröffentlichen die Gesundheitsdaten einiger Patienten. Die Betroffenen beauftragen Spezialisten mit der Löschung der unrechtmäßig veröffentlichten Daten und verlangen vom Arzt Schadenersatz.

- *Schadensersatz: 20.000 Euro nach Art. 82 DSGVO*

Vertrauenskrise

Nachdem die lokale Presse über den Datendiebstahl berichtet, wenden sich zahlreiche Patienten von der Praxis ab, der Patientenstamm schrumpft deutlich.

- *Krisenkommunikation: 1.000 Euro*

Der Umsatzrückgang ist nicht gedeckt

Aufarbeitung

Die Datenschutzbehörden verhängen aufgrund des Datenverlustes ein hohes Bußgeld.

Das Bußgeld ist nicht gedeckt

Musterszenario Ransonware:

Hacker attackieren die IT-Systeme einer Apotheke und sperren die Systeme. Sie wollen die Systeme erst wieder freigeben, wenn sie vom Apotheker Lösegeld bekommen.

Angriff

Die IT-Systeme der Apotheke sind ohne Funktion, auf den Bildschirmen erscheint lediglich die Nachricht der Erpresser.

Austausch der IT-Systeme

Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt der Apotheker kein Lösegeld. IT-Spezialisten suchen und schließen die Schwachstelle, die den Tätern Zugriff zum System erlaubte. Sie setzen neue, sichere Systeme auf und stellen alle Daten der Apotheke aus den Sicherungskopien wieder her.

- *Kosten für IT-Forensik: 5.000 Euro*

Betriebsunterbrechung

Bis die Systeme wieder laufen, bleibt die Apotheke geschlossen. Auch die Abrechnung mit den Krankenkassen ist unmöglich.

- *Kosten für 5 Tage Betriebsunterbrechung: 12.500 Euro*

Vertrauenskrise

Nachdem die lokale Presse vom Cyberangriff erfährt und darüber berichtet, wenden sich zahlreiche Kunden von der Apotheke ab, der Kundenstamm schrumpft deutlich.

- *Krisenkommunikation: 1.000 Euro*

Der Umsatzrückgang ist nicht gedeckt

Diesen Schutz sollten alle haben

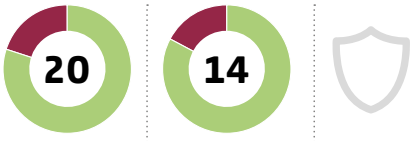
Absolute Sicherheit im Netz gibt es nicht. Doch Widerstand ist möglich. Wer die Gefahren realistisch einschätzt und bei seiner IT-Sicherheit die folgenden Grundlagen beachtet, ist gegen viele Angriffe wirksam geschützt und kann die wirtschaftlichen Folgen eines erfolgreichen Angriffs eindämmen. Die Forsa-Umfrage des GDV zeigt aber: Viele Ärzte und Apotheker haben Lücken in ihrer IT-Sicherheit (Angaben in Prozent).

Der **Cyber-Sicherheits-check des GDV** unter www.gdv.de/cybercheck stellt Ihnen die wichtigsten Fragen rund um Ihre IT-Sicherheit. So finden Sie schnell heraus, wie sicher Ihre Systeme sind, wo Sie Schwachstellen haben und wie Sie diese schließen können. Ob Sie die zehn grundlegenden Anforderungen erfüllen, können Sie gleich hier beantworten.

	Ärzte	Apotheken	Selbsttest
1. Sicherheitsupdates automatisch und zeitnah einspielen und alle Systeme auf dem aktuellen Stand halten Die meiste Software erhält regelmäßig Updates. Sie dienen oft dazu, bekannt gewordene Sicherheitslücken zu schließen. Das Installieren der Updates schützt die Systeme vor Angreifern.	17	5	
2. Mindestens einmal wöchentlich Sicherungskopien machen Daten und digitale Systeme können gezielt angegriffen, versehentlich gelöscht oder durch Hardware zerstört werden. Deshalb ist es dringend nötig, die vorhandenen Daten regelmäßig zu sichern. Grundsätzlich gilt: Je öfter Sie Ihre Daten sichern, desto besser.	18	10	
3. Administratoren-Rechte nur an Administratoren vergeben Wer mit Administratorrechten an einem IT-System arbeitet, kann dabei verheerende Schäden anrichten. Deshalb ist es ratsam, solche Rechte nur sehr sparsam zu vergeben und nur dann zu nutzen, wenn sie für die aktuelle Aufgabe wirklich nötig sind.	20	13	
4. Alle Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, zusätzlich schützen Mobile Geräte können leicht verloren gehen oder gestohlen werden. Sind die darauf gespeicherten Daten nicht verschlüsselt, können sie vollständig ausgelesen werden – selbst wenn sie mit einem Passwort geschützt sind. Server sind über das Internet ständig erreichbar und daher für Angriffe besonders beliebte Ziele. Sie sollten am besten mit einer 2-Faktor-Authentifizierung gesichert werden.	20	14	

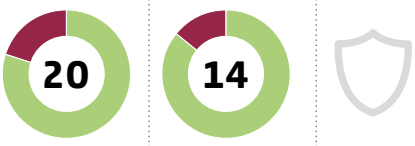
5. Manipulationen und unberechtigten Zugriff auf Sicherungskopien verhindern

Backups sind die Rückversicherung für den Fall gelöschter oder manipulierter Daten. Gesonderte Authentifizierungsstufen und ein entsprechendes Rechtemanagement sollten daher die versehentliche oder absichtliche Manipulation gesicherter Daten ausschließen.



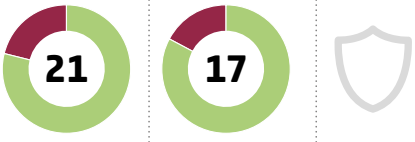
6. Alle Systeme mit einem Schutz gegen Schadsoftware ausstatten und diesen automatisch aktualisieren lassen

Viren, Trojaner oder Ransomware: Die meisten Schäden entstehen durch das unbeabsichtigte Infizieren der Systeme mit so genannter Schadsoftware. Auch wenn Virenscanner hier keinen hundertprozentigen Schutz bieten, sollte mindestens einer auf den Systemen installiert sein und regelmäßig aktualisiert werden.



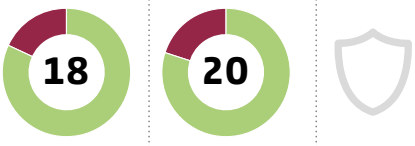
7. Sicherungskopien physisch vom gesicherten System trennen

Datensicherungen können auch dann vor dem Verlust Ihrer Daten schützen, wenn die Systeme gestohlen oder durch einen Brand zerstört wurden. Deshalb ist es ratsam, die Backups nicht in der Nähe der laufenden Systeme aufzubewahren, sondern mindestens in anderen Brandabschnitten, besser jedoch an einem ganz anderen Ort.



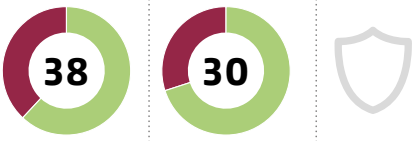
8. Mindestanforderungen für Passwörter (z.B. Länge, Sonderzeichen) verlangen und technisch erzwingen

Gerade wenn Passwörter das einzige Authentifizierungsmittel sind, sollte eine geeignete Passwortstärke technisch erzwungen werden. Andernfalls sind IT-Systeme schon durch einfachste Angriffe gefährdet.



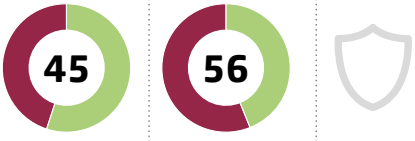
9. Jeden Nutzer mit eigener Zugangskennung und individuellem Passwort ausstatten

Ohne benutzerindividuelle Kennungen ist es nicht möglich, den Zugang zu Systemen zu sichern. Die individuelle Authentifizierung ist auch deswegen wichtig, weil nur so später nachvollzogen werden kann, wer das System wann verwendet hat.



10. Wiederherstellen der Daten aus der Sicherungskopie regelmäßig testen

Regelmäßige Testläufe stellen sicher, dass bei der Sicherungskopie keine Datenquelle fehlt und die Wiederherstellung tatsächlich funktioniert. Der Notfall ist der schlechteste Zeitpunkt um festzustellen, dass eine Sicherungskopie fehlerhaft ist.



Praxen im Praxistest

Wie sicher sind Deutschlands Ärzte wirklich? Der GDV hat einen IT-Spezialisten 25 Arztpraxen auf Herz und Nieren testen lassen – unter anderem eine Zahnarztpraxis in Köln. Ein Livehack.

Hastig schlägt Michael Wiesner in die Tasten seines Laptops. Im Stakkato probiert er immer wieder neue Passwörter aus: „Praxis“, „Behandlung“, „Empfang“. Kryptische Ziffern und Zeichen flackern vor ihm auf dem Bildschirm auf. Nach etwa fünf Minuten grinst Wiesner. Treffer! Er hat das IT-System der Zahnarztpraxis geknackt.

Vor ihm breitet sich die gesamte Ordnerstruktur mit allen Dokumenten aus: Abrechnungen, Termine, Gutachten, Patientenbriefe. Sensibelste Informationen. Würde ein Hacker sie verschlüsseln, käme der Praxisbetrieb zum Erliegen. Wenn die Gesundheitsdaten gestohlen und ins Netz gestellt würden, müsste die Ärztin zudem mit hohen Strafen rechnen. „Es wäre existenzbedrohend, würde ein Krimineller an diese Daten kommen“, sagt die betroffene Medizinerin aus Köln, die ihren Namen nicht öffentlich machen möchte.

> Würde ein Krimineller an diese Daten kommen, wäre das existenzbedrohend

Passwörter sind leicht zu knacken

Würde, hätte, könnte – denn dies ist nur ein Test und Wiesner ein sogenannter White-Hat: ein Hacker, der auf Bestellung IT-Systeme auf Herz und Nieren prüft. Ende 2018 ist er quer durch Deutschland unterwegs, um im Auftrag des GDV 25 Arztpraxen zu testen. Die Mediziner wollen wissen, ob ihre IT-Systeme Sicherheitslücken haben.

Und die findet Wiesner zuhauf – auch wenn es von außen bei den meisten Praxen zunächst vielversprechend aussieht. Tatsächlich ist die Absicherung gegen externe Angriffe auf den ersten Blick gut. Das liegt allerdings weniger an den Ärzten und ihren IT-Dienstleistern, sondern vielmehr an der Hardware: Inzwischen verfügen auch einfache DSL-Router über ausreichende Schutzfunktionen. Und nur selten sind Dienste für einen Zugriff über das Internet freigeschaltet.

Doch die Sicherheit ist trügerisch. Selbst wer kein Genie im

Über den IT-Sicherheitscheck von 25 Arztpraxen

Der GDV hat die IT-Sicherheit von 25 niedergelassenen Ärzten umfassend analysieren lassen. Michael Wiesner, Cyber-Security-Experte aus dem Expertennetzwerk der VdS Schadenverhütung GmbH, testete die technische und organisatorische IT-Sicherheit der 25 freiwilligen Teilnehmer sowohl vor Ort in der Praxis als auch von außen mit Phishing-Mails und einem Penetrationstest. Die teilnehmenden Ärzte rekrutierten sich aus der Leserschaft der ÄrzteZeitung. Die Sicherheitschecks fanden zwischen dem 1. September und dem 31. Dezember 2018 statt.

Programmieren und Hacken ist, findet in vielen Praxen einen einfachen Weg zu sensiblen Daten. Und der führt ganz simpel durch die Eingangstür. Vor Ort in den Arztpraxen wäre es für Cyberkriminelle oft ein Leichtes, sich Zugang zu internen Systemen, Abrechnungen, Gutachten oder gar zu vollständigen Patientenakten zu verschaffen. Frei zugängliche Netzwerkdosen im öffentlichen Bereich der Praxisräume oder nicht abgeschlossene Serverschränke machten es möglich. Doch abseits dieses Leichtsinns seien das größte Problem die viel zu einfachen Passwörter: „Praxis, Behandlung oder die Namen der eingesetzten Arztsoftware sind gängige Kennwörter in den Praxen“, sagt Wiesner. Im Ergebnis bewertet Wiesner das Risiko für einen internen Angriff bei 21 der 25 Praxen als hoch oder sogar sehr hoch. Bei allen Betroffenen hätten Angreifer leichtes Spiel, die Kontrolle über die komplette IT-Infrastruktur zu übernehmen.

Die laschen Schutzvorkehrungen stehen im krassen Widerspruch zu den sensiblen Daten, über die Ärzte verfügen. Und die sie zu einem beliebten Angriffsziel von Hackern machen. Kommen Kriminelle in ihren Besitz, haben sie etwas gegen den Mediziner in der Hand. „Ärzte sind eine gut erpressbare Berufsgruppe, da es mit einem hohen Imageschaden verbunden wäre, wenn die Öffentlichkeit von einem Sicherheitsleck in der Praxis erfahren würde“, sagt Wiesner.

Ärzte unterschätzen Gefahr von Hackerangriffen

Bei vielen Medizinern herrscht indes Sorglosigkeit- und im Alltag viel Stress. Viele scheuen deshalb zusätzliche Hürden, einige Praxen verzichten sogar komplett auf Passwörter. „Wenn dann noch der Server ohne Firewall mit dem Internet verbunden ist, kann jeder im Internet darauf zugreifen – und das ist gar nicht so selten“, urteilt der IT-Sicherheitsberater.

Und auch der Mensch selbst stellt eine große Schwachstelle dar. Häufiges Einfallstor für Hacker sind E-Mails mit Dateianhängen, die Schadprogramme enthalten. Auch Wiesner greift die Arztpraxen mit sogenannten Phishing-Mails an: Die angeblich von einem Arzt-Bewertungsportal stammende Nachricht informiert über eine schlechte Bewertung der Praxis. Für immerhin sechs Ärzte ist das Grund genug, das angehängte Word-Dokument herunterzuladen oder den Link in der Mail anzuklicken. Damit ist ihr System infiziert und der Hacker hätte vollen Zugriff.

Welch gravierende Folgen ein unbedarfter Klick haben kann, hat auch die Kölner Zahnärztin schon erfahren müssen – allerdings nicht bei einem Test, sondern bei einer echten Attacke. Eine Mitarbeiterin hatte den schadhaften Anhang einer fingierten Bewerbungsmail geöffnet und gewährte dem Angreifer →

→ so Zugang zum System. Die Ärztin reagiert schnell. Sie löst den Computer sofort vom Netzwerk und zieht den Stecker. „Der Computer war hinüber, aber das Netzwerk war noch nicht infiziert." Der Vorfall hätte auch schlimmeren Schaden anrichten können, weiß die Medizinerin.

Aus dem Angriff hat sie Konsequenzen gezogen und technisch aufgerüstet. Ihre IT wird regelmäßig gewartet, wie auch Fachmann Wiesner schnell erkennt: „Die Systeme stellen kein kritisches Risiko dar. Das ist ein guter und wichtiger Punkt." Das ist aber keineswegs überall so. Weil Mediziner in der Regel wenig Berührung mit IT-Themen haben, sind sie stark von ihrem IT-Dienstleister abhängig – dessen Qualität sie aber in den wenigsten Fällen tatsächlich beurteilen können. Im Ergebnis bewertet Wiesner die IT-Sicherheit der getesteten Arztpraxen als unterdurchschnittlich. Bei vielen gibt es gute Ansätze, aber Sicherheitslücken finden sich fast überall.

So ist es auch in Köln. Obwohl die Praxis vergleichsweise gut abschneidet, bleibt für die Zahnärztin noch etwas zu tun: „Die Änderung der Zugangspasswörter steht jetzt an erster Stelle. Auch meine privaten Kennwörter werde ich ändern." ←

Dann starten die Angriffswellen

Mit dem Passwort „Praxis" kommt Michael Wiesner in jede zweite Praxis-IT.
Das will der White-Hat-Hacker ändern – und gibt Tipps für eine bessere Informationssicherheit.

Wie gehen Sie vor, wenn Ihnen ein Arzt einen Hacker-Auftrag erteilt?
Michael Wiesner: Tatsächlich schauen wir uns erst mal die äußeren Faktoren an: Wie sind die Türen gesichert, gibt es öffentlich zugängliche Netzwerkdosen, wo steht der Server, sind die PCs gesperrt, wenn niemand daran arbeitet? Wie ist der Zugang aus dem Internet auf die Arztpraxis geschützt?

Anschließend finden wir im Gespräch mit dem Arzt und den Angestellten heraus, welche Sicherheitsroutinen sie einhalten: Wie oft findet eine Datensicherung statt, wie oft wird die Datensicherung getestet? In einem Schwachstellen-Scan finden wir anschließend heraus, wie das Netzwerk und die IT-Systeme gesichert sind. Und dann starten wir die Angriffswellen.

Haben Sie drei Tipps, die jedes Unternehmen sicherer machen?
Wiesner: Ganz übergeordnet muss das Ziel sein, ein vernünftiges Management der Informationssicherheit zu etablieren. Das lässt sich am ehesten erreichen, wenn man die drei größten Schwachstellen versucht zu bekämpfen: Erstens veraltete Systeme, die nicht mehr oder nur noch schlecht zu warten sind. Zweitens die viel zu schwachen Passwörter. Und drittens die fehlende Segmentierung, also Trennung der Netzwerke.

Wie finde ich als Unternehmen einen guten Hacker?
Wiesner: Der beste Weg zum Hacker führt über den Austausch mit anderen Unternehmen, also über Empfehlung. Wir haben in Deutschland mittlerweile eine ganze Reihe sehr guter Dienstleister, die professionell Penetrationstests durchführen und auch bei einem externen Angriff die entsprechende Unterstützung leisten können. ←

Das sind die 5 größten Risikofaktoren

Risiko 1: Passwörter/Zugänge

→ 22 von 25 Praxen nutzen sehr einfach zu erratende Passwörter (z. B. Behandlung, Praxis, Name des Arztes) oder gar keine Passwörter

→ In 22 von 25 Praxen teilen sich mehrere Benutzer dieselbe Zugangskennung

→ In 20 von 25 Praxen haben alle Benutzer Administratorenrechte

→ Keine Praxis prüft, ob alte Administratorenrechte noch bestehen.

Drei Tipps für sichere Passwörter

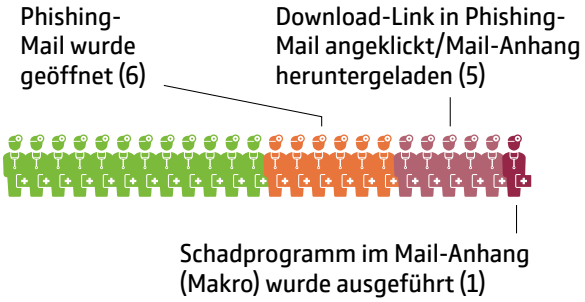
1. Denken Sie sich laaaaaaaange Passwörter aus
Sonderzeichen und Großbuchstaben helfen nur bedingt weiter, ebenso das ständige Wechseln von Passwörtern. Wichtiger ist die Länge. Hacker „raten" Passwörter in der Regel nicht, sondern probieren in kurzer Zeit große Mengen möglicher Kombinationen aus. Je länger das Passwort ist, desto länger braucht auch der Computer. Ein einfaches Beispiel, das Sie bitte nicht direkt verwenden: Um „Pa$$W0rt" zu knacken, braucht ein herkömmlicher PC nach Auskunft der Webseite checkdeinpasswort.de gerade mal sechs Stunden, für „Pa$$W0rt-Hallo123" mehrere Milliarden Jahre.

2. Verwenden Sie einen Passwort-Manager
Sie und Ihre Mitarbeiter können und wollen sich die vielen langen und komplizierten Passwörter nicht merken? Dann fangen Sie auf keinen Fall an, immer das gleiche oder nur ein leicht abgewandeltes Passwort einzugeben. Das macht es Hackern zu einfach. Die bessere Alternative sind Passwort-Manager. Sie generieren und verwalten starke (=lange) Passwörter, die Sie sich nicht merken müssen; das übernimmt der Manager. Da die Anbieter ihre Daten in aller Regel verschlüsseln, sind die Passwörter auch gegen Hackerangriffe geschützt. Sie brauchen für alle Passwörter hingegen nur noch das „Master-Kennwort" – das natürlich wiederum sehr sicher sein sollte.

3. Nutzen Sie die Zwei-Faktor-Authentifizierung
Für den Schutz von Patientendaten sollten Sie ernsthaft eine Zwei-Faktor-Authentifizierung in Betracht ziehen. Das Verfahren kennen Sie von Ihrer Bank: Am Geldautomaten brauchen Sie ihre Giro-Karte (1. Faktor) und die PIN (2. Faktor), auch eine Überweisung beim Online-Banking funktioniert in aller Regel nur mit PIN und TAN. Den Zugang zu Ihren Systemen können Sie genauso schützen – dann bekommen Sie nach der Eingabe Ihres Passwortes zum Beispiel noch einen Code auf Ihr Smartphone geschickt. Alternativ bekommt jeder Mitarbeiter eine Chipkarte, mit der er sich identifizieren kann. Mit dem Passwort allein können Hacker dann nichts mehr anfangen.

Risiko 2: Arglose Mitarbeiter

→ Bei 6 von 25 der attackierten Arztpraxen war der Phishing-Angriff erfolgreich, hier haben die Mitarbeiter auf den in der Mail enthaltenen Link geklickt und das anhängende Word-Dokument heruntergeladen; in einer Praxis wurde sogar das Schadprogramm des Word-Dokuments ausgeführt.



So schützen Sie Ihre Arztpraxis oder Apotheke vor schädlichen E-Mails

Nur ein einziger falscher Klick auf einen verseuchten Mail-Anhang oder einen Link kann die IT-Systeme Ihrer Praxis oder Apotheke lahmlegen. Wenn Sie Ihre Mitarbeiter regelmäßig für die Gefahren sensibilisieren und einige grundlegende Regeln für den Umgang mit E-Mails aufstellen, können Sie sich vor vielen Angriffen schützen.

1. Arbeiten Sie mit hohen Sicherheitseinstellungen
Nutzen Sie die Sicherheitseinstellungen Ihres Betriebssystems und Ihrer Software zu Ihrem Schutz. Im Office-Paket sollten zum Beispiel Makros dauerhaft deaktiviert sein und nur bei Bedarf und im Einzelfall aktiviert werden können – denn auch über diese kleinen Unterprogramme in Word-Dokumenten oder Excel-Listen kann sich Schadsoftware verbreiten.

2. Halten Sie Virenscanner und Firewall immer auf dem neuesten Stand
Die meisten schädlichen E-Mails können Sie mit einem Virenscanner und einer Firewall automatisch herausfiltern lassen. Wirksam geschützt sind Sie aber nur, wenn Sie die Sicherheits-Updates auch schnell installieren.

3. Öffnen Sie E-Mails nicht automatisch
Firewall und Virenscanner erkennen nicht alle schädlichen Mails. Öffnen Sie also nicht gedankenlos jede Mail in Ihrem Posteingang. Erster Schritt: Stellen Sie in Ihrem E-Mail-Programm die „Autovorschau“ aus. So verhindern Sie, dass sich schädliche Mails automatisch öffnen und Viren oder Würmer sofort aktiv werden.

4. Vor dem Öffnen: Prüfen Sie Absender und Betreff
Cyberkriminelle verstecken sich gern hinter seriös wirkenden Absenderadressen. Ist Ihnen der Absender der Mail bekannt? Und wenn ja: Ist der Absender wirklich echt? Achten Sie auf kleine Fehler in der Schreibweise oder ungewöhnliche Domain-Angaben hinter dem @. In betrügerischen E-Mails ist auch der Betreff oft nur unpräzise formuliert, z. B. „Ihre Rechnung“.

5. Öffnen Sie Links und Anhänge nur von wirklich vertrauenswürdigen Mails
Wollen Banken, Behörden oder Kassen sensible Daten wissen? Verweist eine kryptische Mail auf weitere Informationen im Anhang? Dann sollten Sie stutzig werden und auf keinen Fall auf die Mail antworten, Links folgen oder Anhänge öffnen. In Zweifelsfällen fragen Sie beim Absender nach – aber nicht per Mail, sondern am Telefon! Auch eine Google-Suche nach den ersten Sätzen der verdächtigen Mail kann sinnvoll sein – weil Sie so auch Warnungen vor der Betrugsmasche finden.

6. Löschen Sie lieber eine Mail zu viel als eine zu wenig
Erscheint Ihnen eine Mail als nicht glaubwürdig, löschen Sie die Mail aus Ihrem Postfach – und leeren Sie danach auch den Papierkorb Ihres Mailprogramms.

Risiko 3: Datensicherungen sind nur auf den ersten Blick ausreichend

Alle Praxen erstellen mindestens wöchentlich eine Datensicherung....

→ ... aber nur 9 von 25 verschlüsseln ihre Datensicherung

→ ... und nur 4 von 25 testen, ob sich die Daten wiederherstellen lassen

So sichern Sie Ihre Daten richtig

Was? Vom Smartphone bis zum Desktop-Rechner sollten alle Geräte gesichert werden. Kritische Daten sollten besser mehrfach gesichert werden.
Wie oft? So oft und so regelmäßig wie möglich. Stellen Sie am besten mit einem automatisierten Zeitplan sicher, dass keine Lücken entstehen.
Wohin? Speichern Sie das Back-up auf jeden Fall isoliert vom Hauptsystem, also auf einer externen Festplatte, einem Netzwerkspeicher oder in einer Cloud. Kritische Daten sollten auf mindestens zwei unterschiedlichen Speichermedien liegen, von denen eines außerhalb Ihres Unternehmens liegt (z. B. in der Cloud).
Wie aufbewahren? Achten Sie darauf, dass Ihr Back-up nicht mit Ihrem Hauptsystem verbunden ist – weder über Kabel noch über das WLAN.
Was noch? Testen Sie regelmäßig, ob sich die Daten Ihrer Back-ups im Ernstfall auch wirklich wiederherstellen lassen.

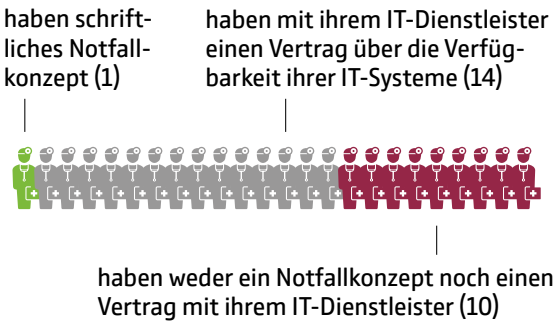
Risiko 4: Fehlende Sicherheitsupdates

→ In 9 von 25 Praxen fehlten aktuelle Sicherheitsupdates der IT-Systeme

Risiko 5: Keine Vorbereitung auf den Notfall

→ Nur 1 der 25 Praxen hat ein schriftliches Notfallkonzept für den Fall eines IT-Ausfalls, die anderen Praxen verlassen sich auf ihren IT-Dienstleister;

→ aber 10 von 25 der Praxen haben keinen entsprechenden Vertrag mit ihrem Dienstleister



Daten sammeln? Klar! – Daten verschlüsseln? Naja.

Eine Analyse der Webseiten und Mailserver zeigt, dass Ärzte, Apotheker und Kliniken beim Datensammeln besser sind als beim Datenschützen. Viele handeln blauäugig.

Den Größen der digitalen Welt bleibt der virtuelle Besuch von Arztpraxen, Apotheken und Kliniken kaum verborgen. Wie eine vom GDV beauftragte Untersuchung zeigt, binden mehr als drei Viertel der Ärzte und Apotheken und zwei Drittel der Kliniken auf ihren Webseiten fremde Inhalte ein. Sie stammen vor allem von Google, Youtube oder Twitter, aber auch das Arztbewertungsportal Jameda oder Xing sind dabei. Der Grund ist klar: Angebote wie etwa Google Maps sind kostenlos und bequem. Patienten finden schnell und einfach ihren Weg zum Arzt oder zur Apotheke. Dass die Patienten dafür aber mit der Preisgabe ihrer Daten bezahlen müssen, ist vielen Akteuren des Gesundheitswesens offenbar entweder nicht bewusst – oder schlicht egal.

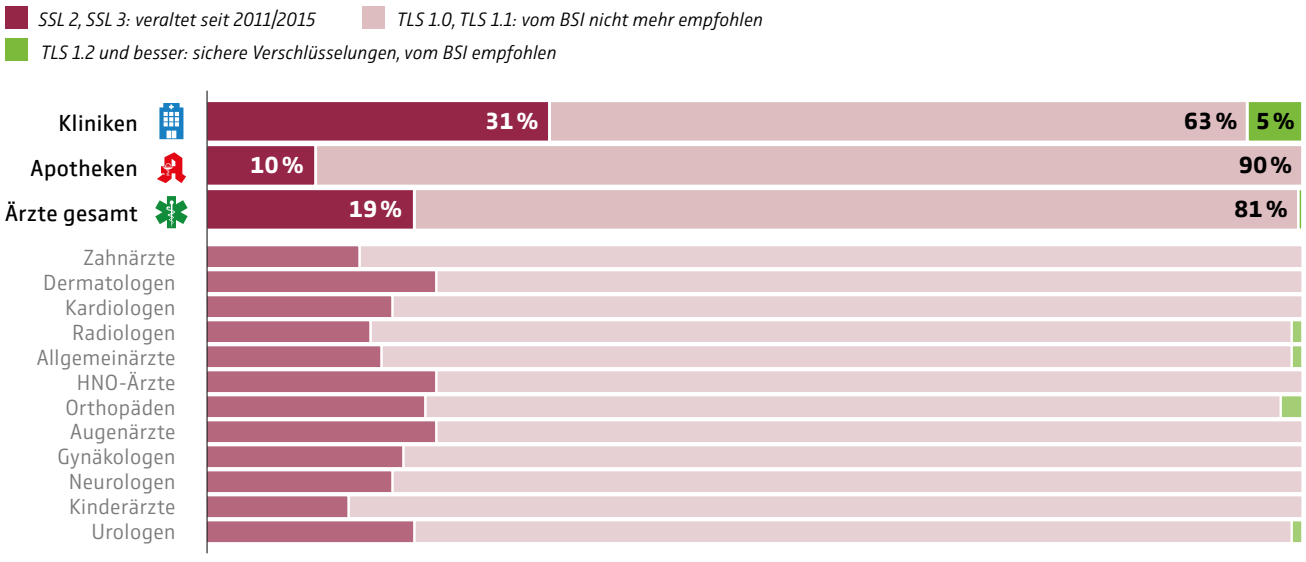
Wer IP-Adressen nicht anonymisiert speichert, verstößt im Zweifel gegen die DSGVO

Großes Interesse an den Daten der Webseiten-Besucher haben aber auch die Betreiber selbst. Egal ob Apotheke, Klinik oder Arztpraxis – rund ein Viertel setzt sogenannte Tracker ein. So können sie feststellen, von welchen Seiten ihre Besucher kommen, wie lange sie auf der Webseite bleiben und was sie sich wie lange ansehen. Tracker schreiben aber nicht nur Aktivitäten auf einer Webseite mit, sondern können Nutzer durch das ganze Internet verfolgen. Besonders problematisch: Teile der untersuchten Webseiten haben die Programme so eingestellt, dass die IP-Adressen der Benutzer nicht anonymisiert werden. Das kann zulässig sein, muss aber in der Datenschutzerklärung klar und korrekt benannt sein. Die Realität sieht in den meisten Fällen anders aus. Die meisten dieser Tracker wurden vor

Über den Cysmo-Sicherheitscheck

Der GDV hat die PPI AG beauftragt, mit Hilfe des Analyse-Tools Cysmo die Sicherheit der IT-Systeme von rund 1.200 niedergelassenen Ärzten verschiedener Fachrichtungen sowie von jeweils rund 250 Apotheken und Kliniken zu testen. Cysmo ist ein vollautomatisiertes Analysetool. Es erfasst und analysiert alle öffentlich einsehbaren Informationen aus Sicht eines Angreifers und kann so potentielle Angriffspunkte aufzeigen. Die Tests fanden zwischen November 2018 und März 2019 statt.

Patientendaten besser nicht per Mail schicken

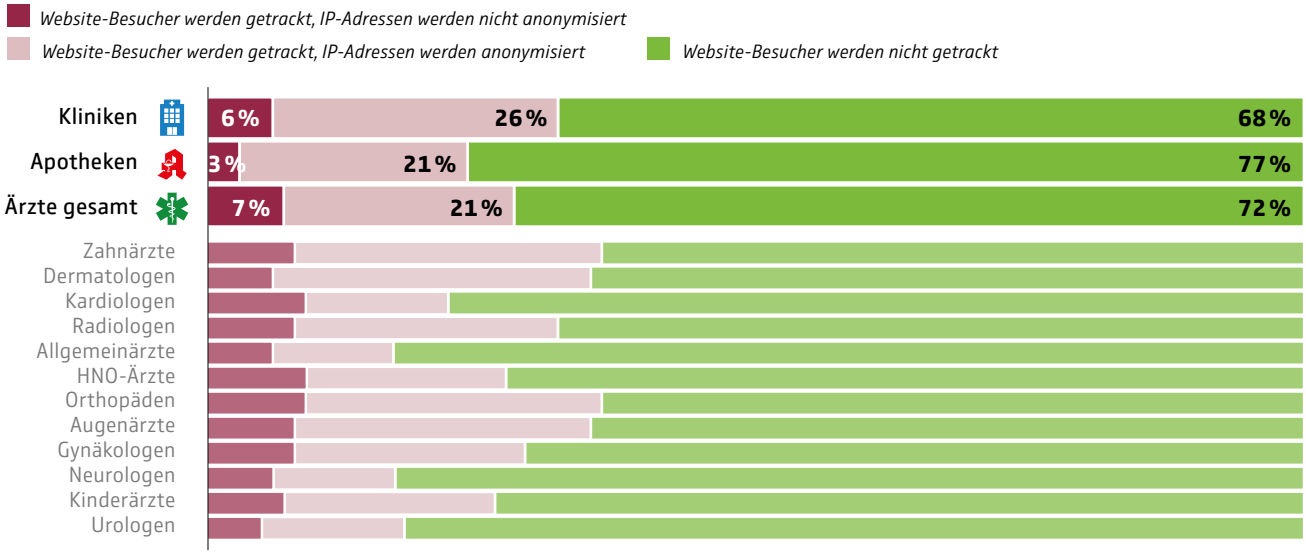


Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) installiert und dann nicht mehr angepasst – in der Regel fehlt in solchen Fällen auch eine korrekte Datenschutzerklärung. Wird ein solcher Verstoß gegen die DSGVO festgestellt, können empfindliche Strafen drohen.

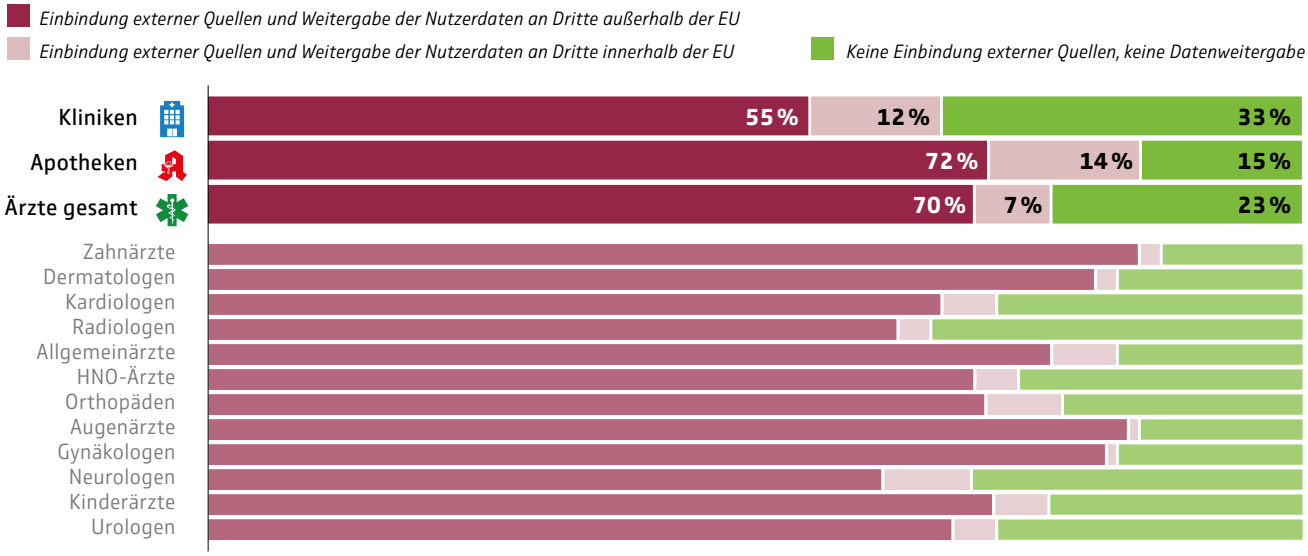
Handlungsbedarf bei der Verschlüsselung von Mails

Ebenfalls nicht auf dem neuesten Stand sind bei den meisten untersuchten Webseiten die unterstützten Verschlüsselungsstandards im Mailverkehr. Viele Mail-Server sind so eingestellt, dass sie noch Verschlüsselungen unterstützen, die schon seit mehreren Jahren veraltet und damit unsicher sind. Die neuesten Verschlüsselungstechnologien und damit einen sehr guten Schutz haben nur die wenigsten, die breite Masse hinkt der Entwicklung hinterher. Hier besteht akuter Handlungsbedarf: Die Verschlüsselungsstandards TLS 1.0 und TLS 1.1 galten noch vor einem Jahr als ausreichend sicher. Doch seit Sommer 2018 werden sie vom Bundesamt für Informationssicherheit (BSI) nicht mehr empfohlen. Die Auswertungen zeigen jedoch, dass die meisten der untersuchten Webseiten hierauf noch nicht reagiert haben. Für Patienten heißt das: Wer intime und vertrauliche Daten wirklich per Mail an einen Arzt oder eine Klinik schicken will, sollte sich nach den Sicherheitsstandards erkundigen – oder doch ein anderes Medium nutzen. ←

Hohes Interesse am Verhalten der Nutzer



Viele Nutzerdaten gehen an Dritte



Ins Licht gezerrt

Wenn Hacker Webseiten und Internetportale knacken, haben sie es häufig auf die Zugangsdaten der Kunden abgesehen. Die Cysmo-Untersuchung zeigt, dass auch die Daten von Arztpraxen, Apotheken und Kliniken betroffen sind – und woher die Daten stammen.

Die Kombination von E-Mail-Adresse und Passwort kann Gold wert sein – denn viele Nutzer sind bequem und nutzen immer dieselben Zugangsdaten für die Anmeldung bei verschiedenen Diensten oder Portalen. Werden diese bekannt, ist es für Angreifer leicht, gleich mehrere Accounts zu kapern. Das kann für die Betroffenen katastrophale Folgen haben. Im Extremfall übernehmen Hacker ganze Identitäten und lassen Waren an eine beliebige Adresse liefern, schließen und kündigen Verträge, erpressen die betroffenen Nutzer oder führen Freunde, Verwandte, Behörden, Arbeitgeber und Patienten in die Irre.

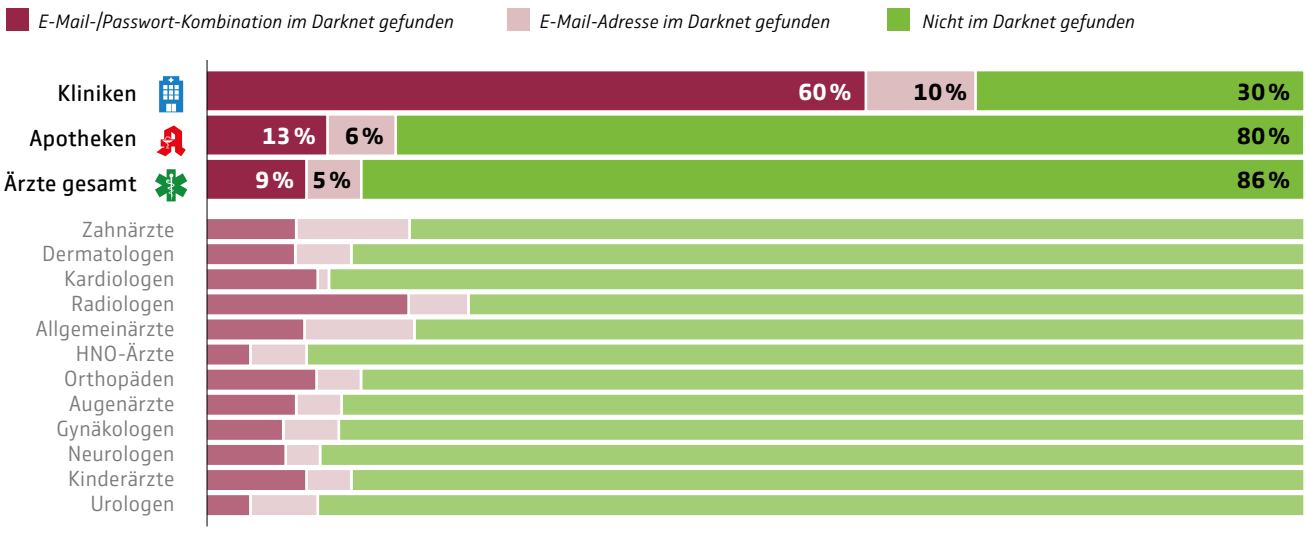
Tauchen Zugangsdaten also im Darknet auf, ist eine schnelle Reaktion gefragt: Die Passwörter sollten umgehend geändert werden, und zwar nicht nur auf der betroffenen Seite, sondern bei allen Zugängen, die mit demselben oder einem ähnlichen Passwort geschützt sind. Wie groß die Sorglosigkeit vieler Mitarbeiter im Gesundheitswesen ist, zeigt die Cysmo-Stichprobe. Mehr als jede zehnte Artzpraxis und Apotheke ist betroffen, unter den Kliniken ist es aufgrund der höheren Mitarbeiterzahl sogar die Mehrheit – allein von einer Klinik fanden sich im Darknet sage und schreibe 185 E-Mail- und Passwort-Kombinationen. Außerdem stellt sich heraus: Viele nutzen ihre beruflichen Mail-Adressen nicht nur im beruflichen Kontext– denn allein in der Stichprobe stammen mehr als 40 Datensätze von einem Hack der Partnerbörse Badoo. ←

Sind Sie betroffen? Hier finden Sie es heraus.

Der Service „Have I Been Pwned?“ (Pwned wird gesprochen wie „poned“) hat über 6 MilliardenDatensätze aus mehr als 300 Datenlecks gesammelt. Wenn Sie überprüfen wollen, ob auch Ihre Mail-Adresse darunter ist, geben Sie diese einfach in der entsprechenden Suchmaske ein, das Ergebnis wird sofort angezeigt. → https://haveibeenpwned.com/

Das Hasso-Plattner-Institut bietet den „HPI Identity Leak Checker“ an. Sie können anhand ihrer E-Mailadresse prüfen, ob die Adresse in Verbindung mit anderen persönlichen Daten wie Geburtsdatum oder Adresse im Internet offengelegt wurde und missbraucht werden könnte. Anders als bei „Have I been Pwned?“ erhalten Sie das Ergebnis per Mail.
→ https://sec.hpi.de/ilc/

Ergiebige Suche im Darknet



Das leistet eine Cyberversicherung

Der Gesamtverband der Deutschen Versicherungswirtschaft hat unverbindliche Musterbedingungen für eine Cyberversicherung entwickelt. Sie sind speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen zugeschnitten und richten sich damit unter anderem an Ärzte und Apotheker. Die Versicherung übernimmt nicht nur die Kosten durch Datendiebstähle, Unterbrechungen des Praxis- bzw. Apothekenbetriebs und für den Schadenersatz an Dritte, sondern steht den Kunden im Ernstfall mit einem umfangreichen Service-Angebot zur Seite. Nach einem erfolgreichen Angriff schickt und bezahlt die Versicherung Experten für IT-Forensik, vermittelt spezialisierte Anwälte und Krisenkommunikatoren. So hilft sie, den Schaden für betroffene Ärzte und Apotheker so gering wie möglich zu halten.

	Schaden	Leistung
Eigenschäden	Wirtschaftliche Schäden durch Unterbrechungen des Praxis- bzw. Apothekenbetriebs	Zahlung eines Tagessatzes
	Kosten der Datenwiederherstellung und System-Rekonstruktion	Übernahme der Kosten
Drittschäden	Schadenersatzforderungen von Patienten wegen Datenmissbrauch	Entschädigung und Abwehr unberechtigter Forderungen
Service-Leistungen	IT-Forensik-Experten zur Analyse, Beweissicherung und Schadenbegrenzung	Jeweils Vermittlung und Kostenübernahme
	Anwälte für IT- und Datenschutzrecht zur Beratung	
	PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens	

Impressum

Herausgeber:
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G
10117 Berlin
Tel. +49 30 2020-5000
berlin@gdv.de, www.gdv.de

V.i.S.d.P.:
Christoph Hardt

Redaktion:
Henning Engelage
Simon Frost
Saraida Höfer
Christian Siemens

Bildnachweis:
S. 1: everything possible
S. 10: Getty Images/ Boonchai Wedmakawand
S. 11: Saraida Höfer
S. 12: Katharina Weber

CYBER SICHER

Eine Initiative der Deutschen Versicherer.
gdv.de/cybersicher

GDV
DIE DEUTSCHEN VERSICHERER

Wilhelmstraße 43 / 43 G
10117 Berlin
Tel. +49 30 2020-5000
Fax +49 30 2020-6000
E-Mail: berlin@gdv.de

51, rue Montoyer
B-1000 Brüssel
Tel. +32 2 28247-30
Fax +49 30 2020-6140
E-Mail: bruessel@gdv.de

www.gdv.de
www.DieVERSiCHERER.de
facebook.com/DieVERSiCHERER.de
Twitter: @gdv_de
www.youtube.com/user/GDVBerlin