

# Ärzte gehen zu nachlässig mit ihren E-Mail-Accounts um

VON BRITTA RAJMANN



Britta Rajmann

Im Grunde ist es jedem Arzt bekannt: E-Mails mit Patientendaten sollten mit neuesten Verschlüsselungsmethoden versehen werden, Passwörter für E-Mail-Accounts dürfen nicht leicht zu erraten sein, Links und Mailanhänge von unbekanntem Absendern sollten nicht geöffnet werden und berufliche E-Mail-Accounts sollten auf keinen Fall privat genutzt werden.

## Oft leicht zu erratende Passwörter gewählt

In der Praxis sieht es jedoch – wie beispielsweise eine repräsentative Forsa-Umfrage zur IT-Sicherheit im Gesundheitssektor im Jahr 2018 offenbart hat – etwas anders aus: Die Befragung, die im Auftrag des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) unter 200 Arztpraxen und 100 Apotheken durchgeführt wurde, ergab, dass die Ärzte in Deutschland häufig zu nachlässig mit ihren Passwörtern umge-

hen. So wählten 90% der befragten Ärzte leicht zu erratende Passwörter wie „Behandlung“ oder ihren eigenen Namen und in ebenso vielen Praxen verwendeten mehrere Benutzer dieselbe Zugangskennung.

## E-Mail- und Passwort-Kombinationen häufig im Darknet zu finden

Eine andere Analyse, die der GDV Ende des Jahres 2018 bei der Softwarefirma PPI in Auftrag gegeben hat, hat ergeben, dass häufig Kombinationen aus E-Mails und Passwörtern von Ärzten im Darknet zu finden sind. Das vollautomatische Analysetool Cysmo hat hierfür bei etwa 1200 niedergelassenen Ärzten und 250 Apotheken und Kliniken untersucht, ob sicherheitsrelevante Informationen öffentlich im Darknet einsehbar sind. Das Ergebnis: E-Mail-Adressen von mehr als 10% der überprüften Arztpraxen waren im Darknet zu finden – praktischerweise mit dem dazugehörigen Passwort versehen. Aufgrund der höheren Mitarbeiterzahl fanden sich bei den überprüften Kliniken sogar bei 60% Mail-Adressen-Passwort-Kombinationen – eine Klinik war sogar mit 185 dieser Kombinationen vertreten. Neben den zu

nachlässig gewählten Passwörtern spielt hier auch eine Rolle, dass viele Nutzer ihre beruflichen Mail-Adressen auch privat einsetzen: Über 40 Datensätze dieser Stichproben wurden in Folge eines Hackerangriffs auf einer Partnerbörse im Darknet veröffentlicht.

Eine Analyse, ob der eigene Mail-Account betroffen ist, wird – so eine Empfehlung des GDL – über die Plattformen „Have I Been Pwned?“ (<https://hveibeenpwned.com>) oder „HPI Identity Leak Checker“ (<https://sec.hpi.de/ilc/>), einem Service des Hasso-Plattner-Instituts, angeboten.

## In jeder zweiten Praxis werden potenziell schädliche E-Mails geöffnet

Auch Tests mit potenziell schädlichen E-Mails zeigen die Sorglosigkeit von Ärzten und ihren Mitarbeitern auf. So überprüfte der Experte in Computersicherheit aus dem Expertennetzwerk der VdS Schadenverhütung, Michael Wiesner, im Auftrag der GDV bundesweit 25 Arztpraxen, indem er potenziell schädliche E-Mails an sie schickte. Die angeblich von einem Arzt-Bewertungsportal stammende Nachricht informiert über eine schlechte Bewertung der Praxis. In

etwa der Hälfte der Praxen wurde die Mail geöffnet, bei etwa 20% wurde sogar ein angehängtes Word-Dokument geöffnet oder auf einen unbekanntem Link geklickt. Hätte es sich um eine echte schädliche E-Mail gehandelt, wären die Empfänger Opfer einer Phishing Attacke geworden, die ihr ganzes System infiziert und dem Hacker vollen Zugriff gewährt hätte: Bei einem derartigen Angriff besteht die Gefahr, dass Patientendaten kopiert und die Systeme der Praxis gesperrt werden. Die Erpresser drohen damit, nur gegen ein Lösegeld auf die Veröffentlichung der sensiblen Daten zu verzichten und die Systeme wieder freizugeben.

## Verschlüsselungsmethoden sind oftmals veraltet

Wie die Überprüfung des Analysetools Cysmo ebenfalls ergeben hat, nutzen fast alle Ärzte und Kliniken Mailserver mit veralteter Verschlüsselung. So verwendeten nur 0,4% der untersuchten 1200 niedergelassenen Ärzte und nur etwa 5% der untersuchten Kliniken die vom Bundesamt für Sicherheit in der Informationstechnik empfohlene sichere Verschlüsselungsmethode. Bei allen anderen werden die Mails mit veralteten Methoden empfangen und verschickt – da diese Mails von außen abgefangen und gelesen werden können, stellt dies eine große Gefahr hinsichtlich der Patientendaten dar.

## Risiko wird unterschätzt

In direktem Gegensatz zu den aufgezeigten Risiken steht die Selbsteinschätzung der Ärzte. So glauben 81% der in der Forsa-Umfrage teilnehmenden Ärzte, ihre Computersysteme seien umfassend geschützt. Oft wiegen sie sich in falscher Sicherheit und nehmen an, dass ihre Daten nicht interessant genug für einen Hackerangriff wären, oder dass die eigene Praxis zu klein sei, um in den Fokus von Hackern zu geraten. Etwa ein Drittel der Teilnehmer plant daher keinerlei weitere Investitionen in die IT-Sicherheit. Wie gefährlich das ist, zeigt die gleiche Umfrage: 78% der Teilnehmer geben an, dass sie im Falle einer Cyberattacke ihre Arbeit einstellen oder stark einschränken müssten – falls ihre Praxis-IT betroffen wäre.

**Der vollständige Branchenreport** „Cyberisiken bei Ärzten und Apotheken“ kann unter folgendem Link nachgelesen werden:



ZEITSCHRIFT FÜR  
PRAKTISCHE AUGENHEILKUNDE &  
AUGENÄRZTLICHE FORTBILDUNG

ISSN 1436-0322

**Herausgeber und Verlag:**  
Dr. Reinhard Kaden Verlag GmbH & Co. KG  
Maafstr. 32/1, 69123 Heidelberg  
Tel. 06221/1377600  
Fax 06221/29910  
info@kaden-verlag.de  
www.kaden-verlag.de

**Schriftleitung:** Dr. med. Annelie Burk  
Bielefeld

**Redaktion:** Dipl. Biol. Ulrike Blumröder  
Heidelberg

**Erscheinungsweise:** 11 Ausgaben pro Jahr  
(monatlich außer August)

**Abonnement:** Bestellung beim Verlag

**Bezugspreis:** Jahresabonnement 110 Euro, für Assistenzärzte in der Weiterbildungszeit bei Vorlage einer Bescheinigung des Arbeitgebers 55 Euro (inklusive 7% MwSt., zuzüglich Porto und Versand). Einzelheft außerhalb des Abonnements 10 Euro / Juli-Heft 21 Euro (inklusive 7% MwSt., zuzüglich Porto und Versand). Der Abonnent kann seine Bestellung innerhalb von 10 Tagen schriftlich beim Kaden Verlag GmbH widerrufen. Die Frist ist gewahrt, wenn der Widerruf rechtzeitig abgesandt wird (Datum des Poststempels). Die digitale ZPA als App ist zusätzlich zum Printabonnement für 14 Euro für 12 Monate erhältlich. Die App alleine für 87,99 Euro. Informationen hierzu unter [www.kaden-verlag.de/abonnement/jetzt-abonnieren/](http://www.kaden-verlag.de/abonnement/jetzt-abonnieren/)

**Bezugszeit:** Das Abonnement gilt zunächst für ein Jahr. Es verlängert sich um jeweils ein Jahr, wenn die Kündigung nicht bis zum 31.10. im Verlag vorliegt. Kann die Zeitschrift aufgrund von Streiks oder höherer Gewalt nicht geliefert werden, so besteht kein Anspruch auf Ersatz.

**Anzeigenannahme:** Durch den Verlag.  
Zur Zeit gilt Anzeigenpreisliste Nr. 40.

**Copyright:** Mit der Annahme eines Manuskriptes erwirbt der Verlag für die Dauer der gesetzlichen Schutzfrist (§ 64 UrhRG) die ausschließlichen Verwertungsrechte im Sinne der §§ 15 ff. des Urheberrechtsgesetzes. Übersetzung, Nachdruck, Vervielfältigung auf fotomechanischem oder ähnlichem Wege, Vortrag, Funk- und Fernsehsendung sowie Speicherung in Datenverarbeitungsanlagen – auch auszugsweise – sind nur mit schriftlicher Genehmigung des Verlages gestattet.

**Layout und Satz:** Alexander Lorenz  
Mannheim

**Herstellung:** Dietz Druck  
Hebelstraße 11, 69115 Heidelberg