Sicherheit von Patient*innendaten

Cybersicherheit und Cyberkriminalität im österreichischen Gesundheitswesen

Wien, März 2022

Durchgeführt im Auftrag von: Dr. Armin Kaltenegger

Sicherheit von Patient*innendaten

Cybersicherheit und Cyberkriminalität im österreichischen Gesundheitswesen

Autor*innen
Dr. Georg Plattner
Anna Teufel, MA
Patricia Jeßner, BA

Mitwirkung
Mag. Dagmar Lehner
David Schwaiger, BSc
Marcus Gabriel, BA
Carl Neumayr, MA

Fachliche Verantwortung
Dr. Georg Plattner

Inhaltsverzeichnis

1. Einleitung

Daten sind ein wertvolles und schützenswertes Gut. Sie tragen Informationen über Individuen, ihre Verhaltensmuster, ihre Vorlieben, aber auch ihre gesundheitlichen Merkmale. Die medizinische Akte eines Menschen ist hochsensibel, nicht umsonst unterliegt diese besonderen Schutzmaßnahmen durch den Gesetzgeber. Durch die Digitalisierung aller gesellschaftlichen Aspekte ist auch die Krankheitsgeschichte eines Menschen digital vorhanden und abgespeichert. So kann schnell und vernetzt auf einen gesundheitlichen Vorfall reagiert werden, der Austausch von Ärzt*innen wurde vereinfacht, und die Behandlung über Fachgebietsgrenzen hinaus kann vereinfacht werden. Hinzu kommt, dass immer mehr Menschen ihre Gesundheitsdaten freiwillig digital speichern und teilen, zum Beispiel über Wearable Devices wie Fitnessuhren.

Gesundheitsdaten existieren also in großer Zahl, sowohl im privaten digitalen Raum als auch im digitalen Gesundheitswesen. Deren Schutz ist ein Thema, das in den letzten Jahren immer mehr an Relevanz gewonnen hat. Mit der Datenschutz-Grundverordnung, kurz DSGVO, wurden Fragen zur Speicherung von Daten und zu deren Schutz in unterschiedlichen Bereichen diskutiert und geregelt. Während die Datensammlung bei der Selbstvermessung optional ist, müssen andere Daten gespeichert werden, etwa um medizinische Behandlungen nachvollziehen und Planungen anstellen zu können. In Krankenhäusern, Ordinationen, Apotheken und bei anderen medizinischen Dienstleistern entstehen große Mengen an Daten. Gesundheitsdaten sind besonders sensibel und weisen grundsätzlich ein hohes Schutzniveau auf – sie sind einmalig und nicht veränderbar.

Gesundheitsdaten sind für Kriminelle von großem Interesse. Sie sind auf dem Schwarzmarkt sehr viel mehr wert als andere personenbezogene Daten, und sie können auch für viele unterschiedliche Dinge eingesetzt werden. Kriminelle können die Daten nutzen, um die Opfer mit Betrügereien oder Scams zu attackieren, die spezifisch auf ihre Krankheitsgeschichte abgestimmt sind. Andererseits können mit diesen Daten auch falsche Versicherungsansprüche erhoben werden, um medizinisches Gerät zu erhalten und anschließend weiterzuverkaufen. Manche Kriminelle nutzen die Daten außerdem, um an verschreibungspflichtige Medikamente zu kommen. Vor allem aber werden gestohlene Gesundheitsdaten in Österreich hauptsächlich dazu verwendet, sehr zielgerichtete Werbung zu organisieren und mit den verkauften Produkten oder Betrügereien Gewinne zu erzielen.

Wie steht es nun aber um den Schutz dieser Daten in Österreich? Dieser Frage haben sich die Plattform Patientensicherheit und das KFV angenommen. Hierbei wurde in einem Methodenmix aus qualitativen Expert*inneninterviews, einer quantitativen Befragung von Gesundheitsbetrieben sowie einem Experiment versucht, unterschiedliche Aspekte dieser hochkomplexen Thematik zu beleuchten.

Die Ergebnisse zeigen, dass Datenschutz in Österreich bereits gut in der Praxis gelebt wird, es jedoch im Bereich Datensicherheit noch sehr viel Luft nach oben gibt. Hier ist es vor allem eine Frage des Zugangs zu Informationen und Unterstützung, die benötigt wird, um die Sicherheit von Patient*innendaten bestmöglich zu gewährleisten.

2. Methoden

2.1. Befragung von Gesundheitsdienstleister*innen

Im Zeitraum von Mitte Juni bis Ende August 2021 wurde ein Fragebogen an verschiedene Kammern und Standesvertretungen versendet, mit der Bitte, diesen über deren Verteiler an ihre jeweiligen Mitglieder weiterzuleiten.

In diesem Zeitraum wurde der Fragebogen von 61 Personen, die als Gesundheitsdienstleister*innen tätig sind, vollständig ausgefüllt. 46 der Befragten arbeiteten in Apotheken, neun in Krankenhäusern, eine Person als niedergelassene*r Ärzt*in, und fünf gaben „andere“ Bereiche an (Hebamme, Psychotherapeut*in etc.).

Tabelle 1: Verteilung der Befragten nach Bundesländern

Bundesland	Anzahl
Burgenland	2
Kärnten	3
Niederösterreich	14
Oberösterreich	12
Salzburg	3
Steiermark	4
Tirol	8
Vorarlberg	1
Wien	14
Gesamt	61

2.2. Expert*inneninterviews

Zusätzlich zu der quantitativen Befragung wurde auch eine Reihe von Expert*inneninterviews geführt. Der Fokus lag hierbei auf dem Status quo von Datenschutz und Datensicherheit im österreichischen Gesundheitswesen. Nachfolgend eine Übersicht über die Interviewpartner*innen.

Tabelle 2: Name und Funktion der interviewten Expert*innen

Name(n)	Funktion	Interview geführt am
Univ.-Prof. Dr. Nikolaus Forgó	Institutsvorstand: Institut für Innovation und Digitalisierung im Recht, Universität Wien	20.07.2021
Mag.[a] Claudia Habl; Dr. Alexander Degelsegger-Márquez	Internationales und Beratung; Digitale Gesundheit und Innovation: Gesundheit Österreich GmbH (GÖG)	21.09.2021
Peter Lenz; Thomas Masicek	Managing Director bzw. Head of Cyber Security: T-Systems Austria & Switzerland	7.10.2021

2.3. Experiment „White-Hat-Hack“

Als dritte Methode wurde das Experiment gewählt. Hierfür wurde ein*e Gesundheitsdienstleistende*r, der*die sich freiwillig am Ende der quantitativen Befragung melden konnte, einem Sicherheitscheck unterzogen. Zu diesem Zweck wurde eine Kooperation mit dem Cybersicherheitsunternehmen Greybox eingegangen, das die Vorbereitung, technische Umsetzung und Nachbereitung des Checks übernahm. Nachfolgend ist schematisch dargestellt, welche Arten von Überprüfungen stattfanden:

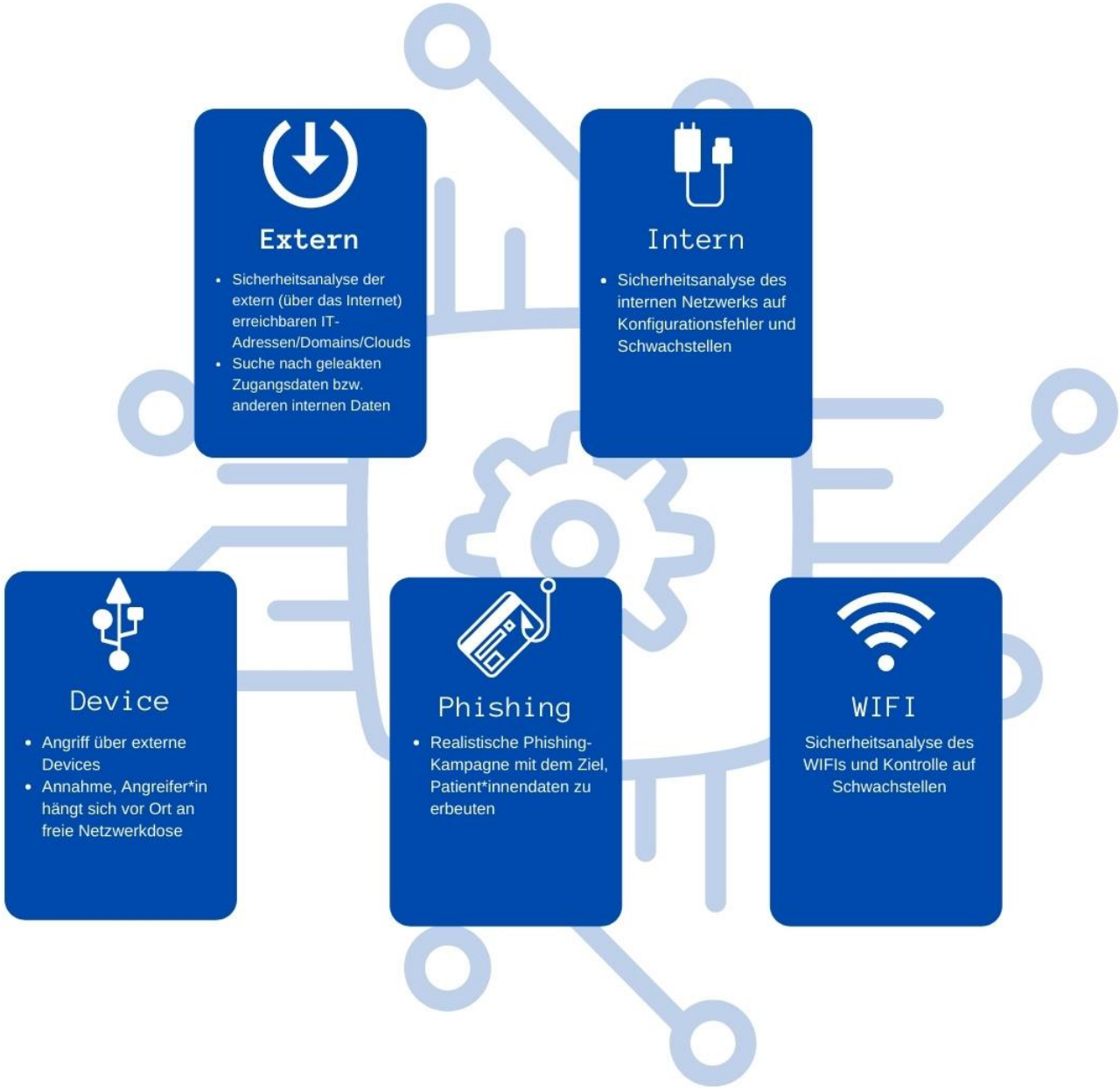

Abbildung 1: Übersicht der durchgeführten Sicherheitsüberprüfungen

3. Relevanz des Themas

Die Sammlung von Daten ist aus den meisten Lebensbereichen nicht mehr wegzudenken. In manchen Bereichen, wie der Medizin, ist diese zwingend notwendig. In anderen, etwa der Selbstvermessung, wird dies aus eigenem Interesse getan. Gesundheits- und Fitness-Apps werden immer beliebter (Kunz, Lange, & Selzer, 2020), vernetzte medizinische Geräte und elektronische Gesundheitsakten ermöglichen eine verbesserte und erleichterte Patient*innenversorgung (Jalali, Russell, Razak, & Gordon, 2019). Dabei werden große Mengen an Daten generiert und gesammelt. Deren Schutz ist ein Thema, das in den letzten Jahren immer mehr an Relevanz gewonnen hat. Mit der DSGVO wurden Fragen zur Speicherung von Daten und zu deren Schutz in unterschiedlichen Bereichen diskutiert und geregelt. Während die Datensammlung bei der Selbstvermessung optional ist, müssen andere Daten gespeichert werden, um beispielsweise medizinische Behandlungen nachvollziehen und Planungen derselben anstellen zu können. In Krankenhäusern, Ordinationen, Apotheken und bei anderen medizinischen Dienstleistern entstehen große Mengen von Patient*innendaten. Gesundheitsdaten sind besonders sensibel und weisen grundsätzlich ein hohes Schutzniveau auf – sie sind einmalig und nicht veränderbar (Lang, et al., 2019). Das Geburtsdatum, die Blutgruppe, die individuelle Krankengeschichte und andere Parameter sind nicht austauschbar und den jeweiligen Personen zugeschrieben. Gesundheitsdaten sind dadurch besonders wertvoll. Je nach Vollständigkeit kann eine Patient*innenakte auf einschlägigen Online-Portalen auf dem Schwarzmarkt zwischen zehn und tausend US-Dollar einbringen (Gordon, et al., 2019).

Generell wird zwischen Datenschutz, dem Schutz von Menschen, deren personenbezogene Daten geschützt werden, und Datensicherheit, dem allgemeinen Schutz der Daten durch technische und organisatorische Maßnahmen, etwa Verschlüsselungsverfahren oder Maßnahmen zur Anonymisierung, zur Verhinderung eines unberechtigten Umgangs mit Daten, unterschieden (Kunz, Lange, & Selzer, 2020). In der DSGVO sind bereits hohe Anforderungen und komplexe Umsetzungsmaßnahmen festgelegt. Dabei ist anzumerken, dass die EU-Regelungen bereits vor der Einführung der DSGVO im internationalen Vergleich betrachtet streng waren. Der österreichischen Gesundheitsbranche ist die Umsetzung der DSGVO sehr gut gelungen, und es gab eine intensive Auseinandersetzung damit.

Digitalisierung hat im Gesundheitswesen – so wie in allen anderen Lebensbereichen auch – Einzug gehalten und ermöglicht bzw. erleichtert die tägliche Arbeit. Das Internet der Dinge (Internet of Things, IoT) ist ein System drahtloser, miteinander verbundener digitaler Geräte, die Daten über ein Netzwerk sammeln, senden und speichern können, ohne dass eine Interaktion von Mensch zu Mensch oder Mensch zu Computer erforderlich ist. Das IoT verspricht viele Vorteile für die Rationalisierung und Verbesserung der Gesundheitsversorgung, um Gesundheitsprobleme proaktiv vorherzusagen und Patient*innen sowohl innerhalb als auch außerhalb des Krankenhauses zu diagnostizieren, zu behandeln und zu überwachen (Kelly, Campbell, Gong, & Scuffham, 2020). Dadurch entstehen große Mengen an digitalen Datensammlungen, die einerseits Vorteile in der Handhabung, Speicherung und Auswertung mit sich bringen, andererseits aber auch ein Sicherheitsrisiko darstellen können (Argaw, Bempong, Eshaya-Chauvin, & Flahault, 2019). Knapp ein Drittel der weltweit gespeicherten digitalen Daten sind

Gesundheitsdaten (Spinazze, Aardoom, Chavannes, & Kasteleyn, 2021). Die Entwicklung der digitalen Patient*innenakten hat in den letzten Jahren deutlich schneller zugenommen als die Entwicklung entsprechender Cybersicherheitsmaßnahmen (Umizeyemungu, Poba-Nzaou, & Cantinotti, 2019).

Krankenhäuser und andere große Gesundheitseinrichtungen sind ein technologiegesättigtes Umfeld. In der Regel verfügen sie im Gegensatz zu anderen Organisationen über wesentlich mehr und unterschiedliche Geräte, die außerdem auf unterschiedliche Patient*innenbedürfnisse ausgerichtet sind. Dazu kommen noch die privaten Geräte, die im Netzwerk der Gesundheitseinrichtungen verwendet werden. Die einzelnen Kliniken und Abteilungen haben jeweils andere Arbeitsabläufe, und der Grad der Spezialisierung ist hoch. Geräte werden meist nicht von einer einzigen IT-Abteilung beschafft, sondern ad hoc gekauft oder von externen Unternehmen kostenlos zur Verfügung gestellt. Das erhöht die Anfälligkeit für Angriffe (Jalali & Kaiser, 2018). Vernetzte medizinische Geräte eröffnen zahlreiche Schwachstellen in der Cybersicherheit eines Krankenhauses. Dennoch werden diese Geräte im gesamten Krankenhaus eingesetzt und können häufig sogar außerhalb des Krankenhauses verwendet werden. Die unterschiedlichen Patient*innenbedürfnisse erfordern häufig Offenheit im Hinblick auf die Interoperabilität von Daten sowie den raschen Zugang zu Gesundheitsakten im Notfall und damit unsichere Codes (Argaw, et al., 2020). In kleineren Ordinationen oder Apotheken fehlt oft das notwendige Hintergrundwissen, welche Daten(schutz)lecks bestehen können und welche Schritte konkret notwendig sind, um ein größtmögliches Maß an Sicherheit zu gewährleisten. Dazu kommt, dass IT-Sicherheit mit hohen Kosten verbunden ist. Die Cybersicherheit im Gesundheitsbereich ist aufgrund der Art der gefährdeten Informationen und der möglichen Folgen für die Patient*innensicherheit außergewöhnlich wichtig (Argaw, et al., 2020; Gordon, et al., 2019).

Während es bei physischen Patient*innenakten noch relativ einfach ist, beispielsweise durch das Versperren eines Aktenschranks, für Sicherheit zu sorgen, ist dies bei der digitalen Speicherung in Clouds oder dem drahtlosen Datentransfer herausfordernder (Kelly, Campbell, Gong, & Scuffham, 2020). Aufgrund der Sensibilität der gesammelten, verarbeiteten und gespeicherten Daten sind Gesundheitsinstitutionen besonders anfällig für Cyberbedrohungen (Widup, Spitler, Hylender, & Bassett, 2018; Jalali, Razak, Gordon, Perakslis, & Madnick, 2019; Williams, Chaturvedi, & Chakravarthy, 2020; Jalali & Kaiser, Cybersecurity in Hospitals: A Systematic, Organizational Perspective, 2018; Argaw, Bempong, Eshaya-Chauvin, & Flahault, 2019; Gordon, et al., 2019). Diese können von der versehentlichen Freigabe von Gesundheitsdaten bis hin zu Störungen der klinischen Versorgung reichen (Argaw, et al., 2020). In diesem Zusammenhang kommt vor allem der Vorbereitung auf einen potenziellen Zwischenfall und der Entwicklung von Plänen für den Ernstfall ein wichtiger Stellenwert zu, zumal keine Organisation – so klein sie auch sein mag – vor einem entsprechenden Angriff gefeit ist (Jalali, Russell, Razak, & Gordon, 2019). Gerade im Gesundheitsbereich ist die Zahl der Angriffe in den letzten Jahren deutlich gestiegen, und dieser zählt weltweit zu den am öftesten attackierten Bereichen (Argaw, et al., 2020).

Eine Studie zur Situation der IT-Sicherheit in europäischen Krankenhäusern zeigt ein beunruhigendes Bild. Im Rahmen dieser Untersuchung wurden Daten der eHealth survey 2013 ausgewertet und fünf grundlegende Sicherheitspraktiken abgefragt: 1) Verschlüsselung der gelagerten Daten, 2) Verschlüsselung der übertragenen Daten, 3) Zugangskontrollen an den

Arbeitsplätzen durch Karten oder Codes, 4) Zertifizierung der Dateneingabe in das IT-System des Krankenhauses mittels digitaler Signatur und 5) die Möglichkeit, im Fall eines vollständigen Datenverlusts im primären Datenzentrum die kritischen klinischen Informationssysteme sofort wiederherzustellen. 13 % der an der Studie teilnehmenden Krankenhäuser gaben an, über keine dieser fünf Sicherheitspraktiken zu verfügen. Verschlüsselung für gespeicherte Daten wird nur in 37 % der Krankenhäuser verwendet. Für übertragene Daten wird sie nur in 59 % der Krankenhäuser eingesetzt. Mehr als 80 % der befragten Krankenhäuser halten es nicht für notwendig, den Zugang zu Arbeitsplätzen mit Gesundheitsdaten durch Ausweise oder Codes des medizinischen Personals zu kontrollieren. Lediglich 18 % der Krankenhäuser haben diese Maßnahmen eingeführt. Krankenhäuser, in denen all diese Maßnahmen nicht umgesetzt werden, setzen Gesundheitsinformationen einer Verletzung der Vertraulichkeit aus (Umizeyemungu, Poba-Nzaou, & Cantinotti, 2019).

Schätzungen gehen davon aus, dass Bedrohungen der Cybersecurity weltweit über alle Branchen hinweg aktuell etwa 6 Billionen US-Dollar pro Jahr kosten (Williams, Chaturvedi, & Chakravarthy, 2020). Für den US-amerikanischen Gesundheitssektor wird der jährliche Schaden auf etwa 6 Milliarden Euro geschätzt (Jalali & Kaiser, 2018). Die COVID-19-Pandemie dürfte dabei potenzierend gewirkt haben: Schätzungen gehen davon aus, dass sich die Zahl der Angriffe dadurch verfünffacht hat (Williams, Chaturvedi, & Chakravarthy, 2020). Gesundheitseinrichtungen können dabei entweder Opfer einer gezielten Attacke sein oder im Rahmen großangelegter internationaler Angriffe wie WannaCry oder NotPetya betroffen sein (Gordon, et al., 2019).

Einer Untersuchung der Unternehmensberatung Roland Berger zufolge waren zwei Drittel der deutschen Krankenhäuser schon einmal Opfer eines Hackerangriffs (Berger, 2017). In 70 % der Fälle waren demografische und sensible Daten betroffen, wobei – wie schon zuvor festgestellt – die Daten im Gesundheitsbereich grundsätzlich sensibel sind. 90 % der Gesundheitsdienstleister waren bereits mit Datenschutzverletzungen (data breach) konfrontiert (Williams, Chaturvedi, & Chakravarthy, 2020), 55 % haben bereits einen Phishing-Angriff erlebt, zumal E-Mail-Adressen relativ leicht herauszufinden oder zu erraten sind und E-Mails von den Empfänger*innen oft auch ohne Kenntnis der Absendeadresse geöffnet werden (Gordon, et al., 2019). Der Gesundheitssektor befindet sich weltweit unter den drei am stärksten von Ransomware betroffenen Branchen, bezüglich Attacken mit bösartiger Computersoftware zählt der Gesundheitssektor zu jenen Zielen, die besonders in den Mittelpunkt der Angriffe gerückt sind (Argaw, Bempong, Eshaya-Chauvin, & Flahault, 2019).

Da die Forschung zeigt, dass der Mensch das schwächste Glied in der Cybersicherheit ist, wird in allen Bereichen betont, wie wichtig es ist, das Bewusstsein der Endnutzer*innen zu schärfen. Sicherheitsmaßnahmen können daher ohne die aktive Beteiligung der verschiedenen Akteur*innen nicht erfolgreich sein. Es braucht regelmäßige Trainings und Schulungen, entsprechende Krisenpläne für den Umgang mit Cyberattacken und das aktive Aufspüren potenzieller Sicherheitslücken, um entsprechend vorbeugen zu können (Argaw, Bempong, Eshaya-Chauvin, & Flahault, 2019; Argaw, et al., 2020).

4. Risiken der Digitalisierung im Gesundheitswesen

4.1. Cyberkriminalität in Österreich: Allgemeines

Cyberkriminalität ist auch in Österreich ein in den letzten Jahren stark gewachsenes Kriminalitätsfeld. Dies zeigt auch die vom Innenministerium im Cybercrime Report 2019 veröffentlichte Anzeigenstatistik: „Die Abbildung der Entwicklung von Cybercrime in den letzten zehn Jahren zeigt, dass mit 28.439 Delikten 2019 gegenüber dem Vorjahr ein Anstieg von 44,9 Prozent zu verzeichnen ist (2018: 19.627)“ (Bundeskriminalamt, 2020, S. 14). Und auch im Vergleich von 2019 mit 2020 zeigt sich erneut ein steiler Anstieg der angezeigten Straftaten.

Die Aufklärungsquote bewegte sich in den letzten drei Jahren stets um die 30 Prozent (siehe auch Abbildung 2). Diese Zahlen fassen jedoch alle Arten von Cyberkriminalität zusammen, sowohl im privaten als auch im wirtschaftlichen Bereich, darüber hinaus auch nur jene, die der engen österreichischen Definition entsprechen.

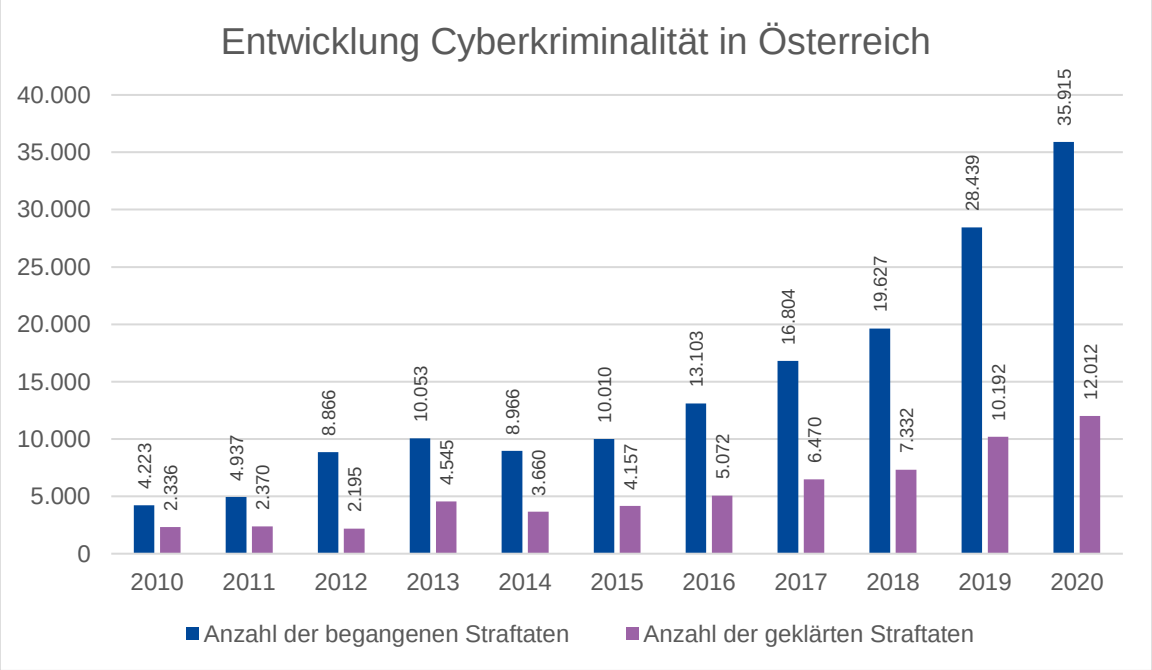

Abbildung 2: Entwicklung der Cyberkriminalität in Österreich. Quelle: Bundeskriminalamt

Die österreichische Gesetzgebung unterscheidet nämlich in ihrer Klassifizierung zwischen Cybercrime „im engeren“ und „im weiteren“ Sinn:

Ersteres bedeutet, wie im obigen Zitat bereits angedeutet, dass sowohl Tatinstrument als auch Angriffsziel IT-Systeme oder Daten sein müssen. Hierfür existiert im Bundeskriminalamt ein spezielles Kompetenzzentrum, das Cyber Crime Competence Center (C4), das als nationale und internationale Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität dient. „2019 musste bei Tatbeständen zu Cybercrime im engeren Sinn ein (…) Anzeigenanstieg von 148,3 Prozent gegenüber dem Vorjahr verzeichnet werden. Die beiden häufigsten Deliktsarten waren

der widerrechtliche Zugriff auf ein Computersystem § 118a Strafgesetzbuch (StGB) und der betrügerische Datenverarbeitungsmissbrauch § 148a StGB“ (Bundeskriminalamt, 2020, S. 15).

Cybercrime im weiteren Sinne bedeutet, dass ein*e Täter*in IT-Systeme zur Tatverwirklichung nutzt, das Ziel jedoch kein IT-System ist. Während unter erstere Definition klassisches Hacking oder auch DDoS-Attacken fallen, fällt unter die zweite Definition die klassische Erpressung (Ransomware) oder Betrug (Phishing), wobei ein IT-System genutzt wird, um eine originär „klassische“ Straftat zu begehen. „Der Internetbetrug (Phishing, Scam, Betrug beim Einkauf im Internet etc., Anm.) erreichte 2019 mit 16.831 Anzeigen einen neuen Höchststand. (…) Auf den gesamten Bereich Cybercrime gerechnet, stellt somit der Internetbetrug etwas mehr als 59 Prozent der Anzeigen dar“ (Bundeskriminalamt, 2020, S. 15 f.).

Die zwei in Österreich am häufigsten auftretenden spezifischen Formen von Cyberkriminalität sind Cyberverbrechen „im weiteren Sinn“:

- Zum einen ist dies Ransomware, also Schadsoftware, die auf IT-Systeme geschleust wird und die darauf befindlichen Daten verschlüsselt. Meist geschieht dies über eine infizierte Datei, die per E-Mail gesendet wird. Die Täter*innen machen sich nun bemerkbar und erpressen ihre Opfer, indem klar gemacht wird, dass die Daten nur gegen Lösegeldzahlungen wieder freigegeben werden. Dies ist vor allem im Wirtschaftsbereich ein großes Problem, weil diese Schadsoftware ganze Produktionsketten zum Erliegen bringen kann.
- Phishing, die zweite massiv steigende Deliktform, ist der Versuch, Geheimdaten abzuziehen. Klassischerweise geschieht dies über eine E-Mail, in der die Adressat*innen aufgefordert werden, ihre Daten auf einer Homepage einzugeben. Dabei wird vorgetäuscht, eine seriöse Institution (bspw. ein anderes Gesundheitsinstitut oder ein Zulieferungsbetrieb) zu sein. Die Seite, die in der E-Mail verlinkt wird, ist meistens täuschend echt nachgebaut und wirkt seriös. Werden die Daten eingegeben, erhalten die Betrüger*innen Zugriff auf das Bankkonto, den Datenserver oder ähnliches.

Diese beiden Delikte steigen auch weiterhin stark an, da sie verhältnismäßig leicht und ohne besondere Vorkenntnisse gesetzt werden können und durch ihren Massencharakter eine sehr große Zahl an potenziellen Opfern in sehr kurzer Zeit erreichen können.

4.2. Spezifische Risiken für Gesundheitsdienstleister*innen

Auch gegenüber Dienstleister*innen im Gesundheitswesen sind es vor allem Phishing und Ransomware, die als Angriffswerkzeuge Krimineller dienen. Damit hebt sich also das Gesundheitswesen zumindest in der Frage der Opferwerdung nur unwesentlich von privaten Bürger*innen ab.

Phishing ist im Gesundheitsbereich ein sehr häufig gewählter Angriffsvektor. Die Kosten für eine täuschend echt aussehende Phishing-Mail sind mittlerweile (auch durch stark verbessertes Maschinenlernen und automatisch generierte E-Mails) gering. Gleichzeitig ist das Gesundheitswesen ein Bereich, in dem Links alltäglich hin- und hergeschickt werden. Eine weitere

E-Mail mit einem Link fällt daher möglicherweise nicht auf. Wird dann dieser Link angeklickt, so öffnet sich eine täuschend echt aussehende Seite, in der dann beispielsweise Zugangsdaten preisgegeben werden. Für den Gesundheitsbereich stellt Phishing ein besonderes Problem dar, vor allem weil die Klickraten im Gesundheitsbereich überdurchschnittlich hoch zu sein scheinen. Der deutsche Cybersicherheitsdienstleister SoSafe führt regelmäßige Phishing-Simulationen durch und stellte fest, dass die durchschnittliche Klickrate allgemein bei 18 % liegt – im Krankenhaus klicken jedoch 23 % der Mitarbeitenden auf den schädlichen Link (Kneip, 2020). Hier sehen Cybersicherheitsexpert*innen vor allem die hohe Arbeitslast in Krankenhäusern mitverantwortlich (Jalali, Bruckes, Westmattelmann, & Schewe, 2020).

Ransomware gehört regelmäßig zu den spektakulärsten und öffentlichkeitswirksamsten Fällen von Cyberkriminalität. Auch hier ist oft eine E-Mail der Anfang. Wie bei Phishing dient die E-Mail vor allem dazu, Vertrauen zu erwecken und Seriosität vorzugaukeln. Die E-Mail enthält meistens jedoch statt eines Links einen Anhang, oftmals ein harmlos wirkendes PDF-Dokument. Wird dieses geöffnet, installiert sich im Hintergrund die Schadsoftware und beginnt ihr Werk. Zunächst sucht die Software nach Daten, die zum Verschlüsseln geeignet sind. Dies geschieht meist unbemerkt, der Eindringling kann durchaus einen längeren Zeitraum „schlafend“ im System bleiben und weiter unauffällig andere Netzwerk-Teile befallen, ohne aktiv zu werden. Die Täter*innen suchen sich einen Zeitpunkt aus, um die Schadsoftware zu aktivieren. Ist dies geschehen, verschlüsselt diese sämtliche Daten, auf die sie Zugriff hat, und es wird eine Erpressungsmeldung eingeblendet. In dieser wird klar gemacht, was passiert ist und wie nun weiter zu verfahren ist. Üblicherweise wird eine Lösegeldzahlung per Bitcoin gefordert, da Überweisungen mit Krypto-Währungen nur schwer nachzuverfolgen sind. Der Preis orientiert sich hierbei an der Unternehmensgröße – idealerweise tut der Preis weh, ohne das Opfer zu überfordern, wie es Thomas Masicek von der Firma T-Systems beschreibt. Im Gesundheitsbereich werden international meist Beträge von 50.000 bis 150.000 Euro (kleinere Praxen) und mehreren Millionen Euro (Krankenhäuser) gefordert, so der Cybersicherheitsexperte (Lenz & Masicek, 2021). In den USA werden laut Schätzungen jährlich mindestens 560 Dienstleister*innen im Gesundheitswesen Opfer von Ransomware (Davis, 2021).

Was passierte bei einigen der spektakulärsten Fälle von Ransomware im Gesundheitswesen? Im Folgenden sollen drei unterschiedliche Fälle exemplarisch vorgestellt werden. In keinem der Fälle ist bekannt, ob die Dienstleister*innen auf die Lösegeldforderungen eingegangen sind. Alle drei hatten mit massiven und langwierigen Ausfällen ihrer digitalen Infrastruktur zu kämpfen, und in allen drei Fällen waren die Ausfälle potenziell oder tatsächlich lebensbedrohlich.

*Im Jahr 2017 wurden weltweit 45.000 Angriffe in 75 Ländern mit der Schadsoftware WannaCry registriert, unter den Opfern waren auch verschiedene Krankenhäuser, unter anderem in England. Die Bevölkerung wurde gebeten, nur in wirklichen Notfällen in die Kliniken zu kommen, einige Patient*innen mussten verlegt werden. Mindestens 6.900 Termine mussten abgesagt werden, der britische Rechnungshof geht gar von bis zu 19.500 ausgefallenen Terminen aus.* (Der Spiegel, 2017; Gesamtverband der Deutschen Versicherungswirtschaft, 2018)

*Im September 2020 wurde die US-amerikanische Krankenhaus-Betreiberin Universal Health Services (UHS) Opfer eines Ransomwareangriffs. Betroffen war eine Vielzahl der 400 Zweigstellen des Unternehmens, der Schaden für das Unternehmen wurde mit 67 Millionen USD beziffert, gerüchteweise starben vier Patient*innen durch den Ausfall der Systeme.* (Davis, 2021)

Im September 2020 wird die Ransomware-Attacke auf das Uniklinikum in Düsseldorf bekannt. Der in das Düsseldorfer Uniklinikum eingeschleuste Erpressungstrojaner verschlüsselt 30 Server und legt nicht nur die IT-Systeme, sondern auch den Notfallbetrieb für 13 Tage lahm. Obwohl die Verschlüsselung schnell aufgehoben wird, dauert es knapp zwei Wochen, bis alle Systeme wiederhergestellt und abgesichert sind. Besonders dramatisch: Dieser langwierige Prozess hat zur Folge, dass eine dringend benötigte Notfallversorgung nicht angeboten werden kann. Die Fahrt in ein deutlich weiter entferntes Krankenhaus in Wuppertal kostet einer Frau das Leben. (Kneip, 2020)

Die Gründe für die Anfälligkeit von Gesundheitsdienstleister*innen sind vielfältig – weiter oben wurde bereits kurz auf den menschlichen Faktor eingegangen: Hohe Arbeitslast, zu hohes Grundvertrauen in die Seriosität eintreffender E-Mails, aber auch nicht ausreichende Schulungen von Mitarbeiter*innen tragen dazu bei, dass im Gesundheitswesen die Datensicherheit nicht immer auf dem höchsten Niveau ist. Zum anderen kommt aber auch hinzu, dass – speziell in kleineren Betrieben und einzelnen Praxen – die IT-Infrastruktur veraltet ist. Thomas Masicek von T-Systems dazu:

> *Wenn man analysiert, wieso es zu solchen Vorfällen im Gesundheitswesen kam, sieht man ganz klar eines, dass zuerst mal die Basics in den Gesundheitsbereichen sehr häufig gefehlt haben. Das heißt, mal beginnend mit einer aktuellen Betriebssysteminfrastruktur, dass ich meine Systeme aktuell halte, dass alle meine Patches installiert sind. Dass ich einen adäquaten Netzwerkschutz habe, sprich, die Zugriffe von außen auf meine Systeme, aber vor allem auch, was darf ich von intern nach außen ins Internet machen, wie darf ich da hinaus kommunizieren? Das ist halt bei sehr vielen Unternehmen, auch im Gesundheitsbereich, nicht gut etabliert. Das Schutzziel der Systemhärtung wurde in diesen Fällen unzureichend umgesetzt, jene der Erkennung und Reaktion waren kaum gegeben.* (Lenz & Masicek, 2021)

Wenn das Ziel jedoch nicht die Bereicherung durch die Erpressung von Lösegeld, sondern der tatsächliche Diebstahl von Patient*innendaten ist, was ist dann der Mehrwert für die Verbrecher*innen? Wie kann man aus diesen sensiblen Daten Profit schlagen?

Zum einen sind die hochsensiblen persönlichen Gesundheitsdaten auf dem Schwarzmarkt sehr viel mehr wert als andere personenbezogene Daten: Einem Bericht des US-amerikanischen Center for Internet Security (CIS) zufolge kosten beispielsweise Kreditkarteninformationen 1-2 US-Dollar auf dem Schwarzmarkt, persönliche Gesundheitsdaten sind jedoch bis zu 363 US-Dollar wert. Dies habe damit zu tun, dass die eigene Gesundheitsakte nicht verändert werden kann, im Gegensatz zu Kreditkartennummern oder der Sozialversicherungsnummer. Kriminelle können diese Daten anschließend nutzen, um die Opfer mit Betrügereien oder Scams zu attackieren, die spezifisch auf ihre Krankheitsgeschichte abgestimmt sind. Andererseits können mit diesen Daten

auch falsche Versicherungsansprüche erhoben werden, um medizinisches Gerät zu erhalten und anschließend weiterzuverkaufen. Manche Kriminelle nutzen die Daten außerdem, um an verschreibungspflichtige Medikamente zu kommen (Center for Internet Security, 2021). Weiters besteht allerdings auch die Möglichkeit, Personen zu erpressen – zum Beispiel, wenn das Opfer eine stigmatisierende Krankheit wie Aids hat, oder gesellschaftlich nach wie vor kontroversielle Thematiken wie Abtreibung oder psychische Krankheiten aus den Daten ersichtlich werden.

Auch Thomas Masicek von T-Systems sieht den Wert gestohlener Patient*innendaten unter anderem in der Möglichkeit der illegalen Beschaffung von Medikamenten (Lenz & Masicek, 2021). Vor allem aber werden die Daten laut Masicek derzeit hauptsächlich dazu verwendet, sehr zielgerichtete Werbung zu organisieren und mit den verkauften Produkten oder Betrügereien Gewinne zu erzielen.

4.3. Präventionsmöglichkeiten

Zu den wichtigsten Präventionsmöglichkeiten in puncto Diebstahl von Patient*innendaten zählt die Verschlüsselung der Daten im Zuge der Speicherung. Dabei sollten verschlüsselte Laufwerke verwendet werden, um es einem potenziellen Eindringling so schwer wie möglich zu machen, Zugriff zu erhalten. Hierzu zählt aber auch, dass die Kommunikation zwischen Dienstleister*innen, aber auch zum Beispiel die Kommunikation mit Krankenkassen, immer verschlüsselt abläuft. Wie in Kapitel 3 bereits angeschnitten, ist dies ein Bereich, der definitiv noch verbesserungswürdig ist (Center for Internet Security, 2021).

Ein weiterer zentraler Punkt der Prävention ist ein einheitliches Protokoll für das Verhalten von Mitarbeiter*innen am Arbeitsplatz und speziell an Systemen, in denen Daten gespeichert sind. Hier wäre es laut Thomas Masicek auch vernünftig, unterschiedliche Berechtigungsstufen für die Mitarbeitenden zu schaffen: Jede Person soll nur jene Zugriffsrechte haben, die sie unbedingt benötigt. So minimiert man das Risiko, dass ungeschultes Personal mit Datensätzen hantiert, die für den eigenen Arbeitsbereich unerheblich sind (Lenz & Masicek, 2021).

Der dritte wichtige Punkt betrifft die Datensicherung: Sollte es zu einem erfolgreichen Ransomware-Angriff kommen, muss der Betrieb in der Lage sein, die Daten wieder zu restaurieren. Ein essenzielles Backup- und Recovery-Konzept kann im Worst Case das Allerschlimmste – den längerfristigen Ausfall der Systeme und den Verlust der Daten – verhindern.

Den letzten wichtigen Punkt bezeichnet Masicek als die „Absicherung meiner Infrastruktur“. Hierfür benötige man aufgrund der Komplexität ein Partnerunternehmen aus der IT-Sicherheitsbranche. Zu diesem Zweck gebe es mittlerweile fertige All-in-one-Pakete, die von der Netzwerkabsicherung bis zum individuellen Arbeitsplatz alles abdecken. „Sich einzelne Bausteine selbst zusammenzuzimmern“, sieht Masicek als wenig effizient an, hier würde dann im Ernstfall auch die Reaktionsfähigkeit fehlen (Lenz & Masicek, 2021).

5. Forschungsergebnisse

5.1. Daten sind geschützt, jedoch nicht immer sicher: Expert*innen zu Datenschutz und Datensicherheit

5.1.1. Datenschutz in Österreich: Die DSGVO als gut eingestellte Benchmark

Geltendes Recht für die Verarbeitung personenbezogener Daten in Österreich sind die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) sowie das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 165/1999.

Personenbezogene Daten sind all jene, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Z 1 DSGVO). U.a. werden **Gesundheitsdaten** als **„besondere Kategorie personenbezogener Daten“** gem. Art. 9 Abs 1 DSGVO eingeordnet. Dazu zählen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren – früheren, gegenwärtigen und künftigen körperlichen oder geistigen – Gesundheitszustand hervorgehen (ErwG 35 sowie Art. 4 Z 15 DSGVO).

Diesen Daten kommt aufgrund der Sensibilität ein besonderer Schutz zu: Die Verarbeitung ist **grundsätzlich verboten**, sofern nicht die **Ausnahmen** nach Art. 9 Abs 2 DSGVO vorliegen. Neben der ausdrücklichen Einwilligung in die Verarbeitung ist diese bspw. dann zulässig, wenn erhebliches öffentliches Interesse besteht, zum Schutz lebenswichtiger Interessen, für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin, der Beurteilung der Arbeitsfähigkeit des Beschäftigten, der medizinischen Diagnostik, der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich und der Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich, oder auch aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit.

Für die Verarbeitung gelten alle gesetzlichen Grundsätze der Art 5 ff DSGVO, wie insbesondere Verarbeitung nach Rechtmäßigkeit, Treu und Glauben und Transparenz, Zweckbindung, Minimierung der Daten, Speicherbegrenzung und Integrität und Vertraulichkeit sowie die Wahrung der Betroffenenrechte. Verantwortliche haben die Sicherheit der verarbeiteten Daten zu gewährleisten und entsprechende technische und organisatorische Maßnahmen umzusetzen (Art 32 DSGVO). Insbesondere zu beachten sind die strengen Meldeverpflichtungen im Falle eines Datenlecks (Meldung an die Datenschutzbehörde binnen 72 Stunden und ggf. Information der Betroffenen, Art 33f DSGVO). Bezüglich der Sicherheit personenbezogener (Gesundheits-)Daten gilt es ein angemessenes Schutzniveau und hierbei insbesondere den branchenüblichen Standard einzuhalten, um nicht Strafen der Behörde bzw. Schadenersatzansprüchen ausgesetzt zu sein.

Auch die Implementierung eines*r Datenschutzbeauftragten kann für kleinere Ordinationen durchaus sinnvoll sein, für größere verbundene Ordinationen/Institutionen bspw. ist diese Position ohnehin idR verpflichtend (so auch Forgó, 2021). Die beauftragte Person steht dem*r Verantwortlichen als unabhängige*r und weisungsfreie*r Berater*in zur Verfügung und fungiert als Informationsschnittstelle zu Betroffenen oder auch zur Datenschutzbehörde.

5.1.2. Cybersicherheit und Datensicherheit: Luft nach oben

Seit Inkrafttreten der DSGVO im Jahr 2018 muss jede Datenverarbeitung in allen EU-Mitgliedsstaaten dieser Rechtslage entsprechen. Als Vorläufer der DSGVO waren personenbezogene Daten, insbesondere auch sensible Daten, in der Datenschutz-Richtlinie 1995 (RL **95**/46/EG) und im DSG 2000 bereits gut und auf hohem Niveau geschützt. Lediglich hinsichtlich des Problembewusstseins gab es in der Vergangenheit allerdings noch Schwierigkeiten. „[D]as Bewusstsein dafür, dass es wirklich auch so gelebt wurde, in allen Institutionen in Österreich, das ist ein Paar Schuhe, das kann man hinterfragen. Aber der Rechtsrahmen war in Österreich immer schon ein sehr starker“ (Habl & Degelsegger-Márquez, 2021). Mit der Einführung der DSGVO kamen einerseits relativ strenge Meldeverpflichtungen und andererseits höhere Strafen bei Verstößen hinzu. Diese führten im Großen und Ganzen zur besseren Einhaltung der geltenden Regelungen und Standards des Datenschutzrechts. „Also das heißt, es ist als Thema stärker in den Köpfen auch der Führungsebene angekommen als davor. Nicht so sehr, weil es sich rechtlich wahnsinnig weiterentwickelt hätte, sondern weil man Strafen stärker als bis dahin betont hat“ (Forgó, 2021).

Laut Forgó sind das Bewusstsein der Ärzt*innen für das angemessene Schutzniveau der Daten im Rahmen ihrer Tätigkeit und die Sensibilität im Umgang mit diesen Fragen in den letzten Jahren deutlich gewachsen. „Und eigentlich, glaube ich, ist man da auf einem guten Weg. Also ich bin da eigentlich sehr viel optimistischer als in vielen anderen datenschutzrechtlichen Bereichen“ (Forgó, 2021). Hinsichtlich Sensibilität besteht laut Forgó aber immer noch Luft nach oben, und es gibt hier dennoch eine Lücke. Um mit den europäischen Standards auch in Österreich mithalten zu können, gibt es beispielsweise großangelegte Cybersecurity-Übungen und Projekte, die sich unter anderem auch mit Datensicherheitsfragen im Gesundheitsbereich beschäftigen (z.B. X-eHealth Projekt).

Hinsichtlich Cyberangriffen werden von der Firma T-Systems derzeit häufig Verschlüsselungsverbrechen registriert, bei denen sich professionelle Gruppen auf die Verschlüsselung von Unternehmen oder Organisationen spezialisiert haben. Dabei geht es hauptsächlich um kommerzielle und weniger um spezifische Dateninteressen. Forgó weist aber auch darauf hin, dass die Kenntnis über den Gegner sehr gering ist. Thomas Masicek von T-Systems nennt drei Szenarien, die für die Patient*innen im Hinblick auf Cyberattacken ein sehr großes Risiko darstellen. Diese sind zum Ersten die Nichtverfügbarkeit der Daten aufgrund einer Ransomware-Attacke. Bereits zu Beginn wurde darauf eingegangen, dass im medizinischen Bereich Daten gesammelt werden müssen, um Behandlungen planen und evaluieren zu können. Wenn der Zugriff auf diese Daten fehlt, stellt das die Gesundheitsdienstleistenden vor ein Problem. Es gibt zwar für diese Fälle Backout-Szenarien, dennoch ist bei einem solchen Vorfall die Leistungsfähigkeit entsprechend eingeschränkt, und das kann eine adäquate Versorgung gefährden. Wenn Daten verschlüsselt oder gestohlen und wieder herausgegeben wurden, stellt

sich zum Zweiten die Frage der Authentizität, d.h., sind die Daten noch integer oder wurden sie verändert? Drittens können die Daten bei einem solchen Angriff entwendet werden und in falsche Hände gelangen. Die dabei erbeuteten Daten werden in der Folge entweder zum Verkauf angeboten oder es wird eine Erpressung versucht. „Wir erleben in den letzten zwei bis drei Jahren sehr stark auch dementsprechend Aktivität der kriminellen Organisationen, die auch natürlich überall dort eingreifen, wo die Wahrscheinlichkeit hoch ist, dass ich entweder sehr wertvolle Informationen erbeuten kann oder damit relativ viel verdienen kann, sprich Erpressung. Und beides trifft aus meiner Sicht auch klar auf den Gesundheitsbereich zu“ (Lenz & Masicek, 2021).

Bei jenen Vorfällen, die in der Vergangenheit passiert sind, fällt auf, dass – wie in Kapitel 4.2. bereits erwähnt – die Grundlagen betreffend Netzwerkschutz und Regeln hinsichtlich der internen und externen Kommunikation nicht gut genug ausgebaut sind. Besonders einfach und daher üblich sind Angriffe via E-Mails, weshalb insbesondere die Kommunikation und Übertragung von medizinischen Daten verschlüsselt erfolgen sollte. Eine Schulung der Mitarbeiter*innen kann in diesem Fall ebenfalls helfen, um potenziell gefährliche E-Mails schon vorab zu erkennen. Auch die Absicherung der Arbeitsplätze ist wichtig, um Angriffe frühzeitig erkennen und entsprechend reagieren zu können. Diese Maßnahmen tragen dazu bei, die Eintrittswahrscheinlichkeit solcher Szenarien zu reduzieren. Insbesondere kleinere Ordinationen im niedergelassenen Bereich sind gefährdet, da dort häufig Standardrechner im Einsatz sind, die „in der Regel nicht gut gewartet und dementsprechend auch in Kombination mit nicht geschulten Mitarbeiterinnen und Mitarbeitern sehr anfällig auf solche Phishing Attacken [sind]“ (Lenz & Masicek, 2021). Dazu kommt in der Regel eine unzureichende Schulung der Mitarbeiter*innen. Das frühzeitige Erkennen eines Angriffs führt meist dazu, dass dieser verhindert werden kann. Dafür braucht es allerdings das nötige Know-how. Doch nicht nur die Einzelnen spielen hier für Masicek eine Rolle, „gefordert [ist auch] die Industrie, hier einfachere Lösungen zu entwickeln, die dementsprechend nicht so einen hohen Aufwand brauchen, den sich bisher nur Großkonzerne leisten konnten. Das heißt, du musst einfach dieselbe Sicherheit, die sich bisher nur Konzerne leisten konnten, bis in eine Ordination bringen. Um dann auch einen wirklich guten Schutz der entsprechenden Patientendaten gewährleisten zu können“ (Lenz & Masicek, 2021). Das Fehlen solcher Erkennungssysteme ist auch dann problematisch, wenn es darum geht, den Angriff zu rekonstruieren, um herauszufinden, was tatsächlich passiert ist, wo die Sicherheitslücke bestanden hat und ob die Daten lediglich verschlüsselt oder auch verändert wurden.

Krankenhäuser sind durch ihre Organisationsgröße deutlich von Ordinationen im niedergelassenen Bereich zu unterscheiden. Diese haben einerseits häufiger Überwachungssysteme, und andererseits sind sie gewachsene und relativ alte Systeme, die nicht miteinander vernetzt sind. Diese „Stand-alone-Systeme“ machen es „schwierig, den Austausch zu garantieren oder einen Verbund zu erstellen. Aber man ist ein bisschen geschützt, weil das sozusagen so autonome oder autarke Systeme sind“ (Habl & Degelsegger-Márquez, 2021). Dennoch stellt Masicek von T-Systems fest: „Was wir sagen können, wir haben einige Krankenhäuser, für die wir auch Überwachungssysteme betreiben, dass wir solche Angriffe laufend dementsprechend auch sehen. Und wie schon gesagt, im niedergelassenen Bereich gibt es solche Vorfälle immer wieder“ (Lenz & Masicek, 2021).

Sowohl seitens der GÖG als auch seitens T-Systems wird dem ELGA-System eine gute Datensicherheit attestiert. Das GINA-Netz, über das die Patient*innendaten übermittelt werden und in dem die e-Card eingebunden ist, ist ein separates System mit eigenen Routern und eigenen Zugängen, das außerdem nicht mit dem Internet verbunden ist. In den einzelnen Gesundheitseinrichtungen beginnt das Sicherheitskonzept jedoch bereits lang vor den hoch technischen Fragen, beispielsweise bei Regelungen und Vorgaben bezüglich der Positionierung eines Monitors oder dem Umgang mit Dokumenten. Im Großen und Ganzen gilt hier: Je größer die Unternehmen, desto strikter und detaillierter die Sicherheitskonzepte, und es gibt eigens bestimmte Verantwortliche für diese Themen. „Das heißt, hier muss man sagen, im größeren Bereich ist das gut umgesetzt. Dort gibt es auch in der Regel aktualisierte Systeme, aktuelle Antivirensoftware, da werden Schutzsysteme etabliert. Dort muss man sagen, hat man sicher eine sehr gute Infrastruktur, die man dementsprechend vorweisen kann (…). Im niedergelassenen Bereich ist das abhängig von den IT-Dienstleistern. Der Arzt hat sein Kerngeschäft, die Medizin, und nicht dafür Sorge zu tragen, dass sein Equipment dort sicher ist. Wohlwissend, dass es in seiner Verantwortung wäre, es zu organisieren“ (Lenz & Masicek, 2021).

„Anfangs hat die Wirtschaftskammer sehr viele Informationen, wie die DSGVO neu war, zur Verfügung gestellt, sehr gute Leitfäden, wo man mal generell ein Bewusstsein schafft dafür eben, wovon rede ich und was ist die Thematik, von welchen Restriktionen bin ich potenziell bedroht. Was haben die Patienten für Rechte, was habe ich als Datenverarbeiter für Rechte und Pflichten“ (Habl & Degelsegger-Márquez, 2021). Themen, die es diesbezüglich zu klären gäbe, sind beispielsweise, ob es ein Dokument gibt, das das Verhalten der Mitarbeiter*innen in der Ordination betrifft und regelt, wer was darf. Es ist auch notwendig, dass unterschiedliche Berechtigungen bezüglich des Zugangs zu und Umgangs mit Patient*innendaten vergeben werden – je nachdem, welcher Zugang für die operative Arbeit notwendig ist. Fragen nach der Datensicherung und nach einer möglichen Wiederherstellung der Daten, für den Fall eines geglückten Angriffs, sollten ebenfalls berücksichtigt werden, und die Infrastruktur sollte technisch abgesichert sein. Ebenso im Vorfeld sollte geklärt werden, an wen man sich wenden kann, falls es doch zu einem Datensicherheitsproblem kommt. „Und da muss man sagen, das ist mittlerweile für einen Arzt, außer, er hat eine IT-Vorbildung, zu komplex. Da braucht man in der Regel einen Partner, der das gemeinsam mit einem macht. Da gibt es mittlerweile auch (…) fertige All-in-one-Pakete, wo ich wirklich von der Netzwerkabsicherung bis hin zu den Arbeitsplätzen alles habe (…). Denn einzelne Bausteine sich selbst zusammenzuzimmern, das ist heute nicht mehr effizient“ (Lenz & Masicek, 2021). Auch Forgó plädiert dafür, auf bestehende Angebote von Expert*innen zurückzugreifen: „Also, Daumenregel für einen irgendwo, seine Praxis absichernd wollenden Arzt oder Ärztin, ist, besser nicht selber machen, besser jemanden nehmen, der das für die Branche schon bisher nachgewiesenermaßen macht. Besser dort ein Produkt nehmen und dann ist man damit meistens zumindest nicht komplett daneben […]“ (Forgó, 2021).

Die meisten Informationen der Branchenverbände sind nach Ansicht von Masicek auf einer sehr hohen Meta-Ebene angesiedelt und zu abstrakt formuliert, vor allem was die technische Infrastruktur betrifft und wofür ein entsprechendes Hintergrundwissen notwendig ist.

Der Großteil der Vorfälle (80 %) betrifft Ransomware. Dabei geht es weniger um ein spezielles Problem von Gesundheitseinrichtungen. Kriminelle Organisationen kaufen E-Mail-Adressen und

versenden Millionen von Phishing-E-Mails in dem Wissen, dass irgendjemand darauf klicken wird. „Hat der Angreifer Zugriff auf das eine System, verschafft er sich Zugriff auf das ganze Netzwerk. Schaut, was für ihn nutzbringend ist. Denn alles, was ich habe, kann ich weiterverkaufen oder ich verschlüssle das Netz. Und was auch immer gemacht wird, ist, dass zusätzlich noch versucht wird, Backups zu löschen, um die Wiederherstellung unmöglich zu machen. Und viele Unternehmen, somit auch dementsprechend die kleineren Ordinationen, arbeiten mittlerweile, weil es komfortabler ist, mit Online-Backups. (…) eine Online-Sicherung ist, wenn ich Zugriff auf die Infrastruktur habe, auch schnell gelöscht. Und somit bin ich gezwungen, entweder von null auf zu beginnen, oder die Ransom zu bezahlen. Das ist derzeit, muss man ganz klar sagen, derzeit noch einer der Hauptvorfälle, dementsprechend auch im Bereich des Gesundheitswesens“ (Lenz & Masicek, 2021).

Die Summen, die in Folge eines solchen Angriffs bezahlt werden, sind variabel, wobei davon auszugehen ist, dass diese so gewählt werden, dass die Betroffenen diese gerade noch bezahlen können bzw. diese Summen den Kosten für den Wiederherstellungsaufwand, also für den notwendigen Aufbau einer neuen IT-Infrastruktur, entsprechen würden. Wenn eine solche Attacke passiert ist, müsste die IT entsprechend erneuert werden, um einerseits für zukünftige Angriffe gewappnet zu sein und um andererseits sicher zu sein, dass die Hacker nicht sogenannte „left-overs“ im System hinterlassen haben, um erneut auf das System zugreifen zu können. Neuerdings bieten die Angreifer*innen häufig einen Nachweis an, dass die Daten nach Bezahlung der Erpressungssumme tatsächlich gelöscht wurden, und/oder ihre Mithilfe bei der Behebung der Schwachstellen im System. „Umso kleiner ein Unternehmen ist, umso häufiger, das kann man auch sagen, wird bezahlt. Also, man kann keine Pauschalsumme sagen, man kann sagen, umso größer ein Unternehmen ist, umso größer ist die Wahrscheinlichkeit, dass, wenn ich verschlüsselt worden bin, einen Weg finden kann, meine Daten dementsprechend wieder herzustellen. Aber ich sage mal, im kleineren Umfeld liegt man hier schon jenseits der 50 Prozent, die bezahlen, so aus Erfahrung“ (Lenz & Masicek, 2021).

Gesundheitseinrichtungen sind aus einem Grund allerdings besonders vulnerable Ziele, wenngleich nicht immer die Gesundheitsdaten an sich im Fokus der Hacker stehen: „Daten sind das neue Gold. Und dementsprechend Daten, gerade Gesundheitsdaten, kann ich teilweise wirklich sehr teuer auch am Markt verkaufen. Umso besser angereichert ein Datum ist mit Personenbezug oder Gesundheitsdaten, damit kann ich sehr viel Geld verdienen. Daher ist das ein sehr gutes Geschäftsmodell, diese Daten auch zu stehlen. Und dann auch weiter zu verkaufen. Was auch immer der Käufer damit macht. Aber der primäre Zweck ist in dem Fall ein kommerzieller Hintergrund“ (Lenz & Masicek, 2021). Personenbezogene Daten sind – je stärker angereichert, desto besser – ein wertvolles Instrument. Die Möglichkeiten gehen hier vom Einsatz gezielter Werbung bis hin zur Identitätsübernahme einer Person.

Luft nach oben in Sachen Datensicherheit sieht Masicek vor allem im niedergelassenen Bereich, wenn es darum geht, das grundsätzliche Schutzniveau anzuheben. Verbesserungen sind in diesem Fall deutlich merklich, da es sich hier um das „übliche Einfallstor“ handelt und die Gesundheitsdienstleister*innen damit bereits einen erheblichen Schritt in Richtung Datensicherheit gehen können. Auch verpflichtende Mindeststandards, die spezifisch

beschreiben, was im Fall des Falles zu tun ist, wären sinnvoll. Diese sind in den großen Gesundheitseinrichtungen bereits üblich, im niedergelassenen Bereich allerdings noch nicht Usus.

5.2. Selbstwahrnehmung von Gesundheitsdienstleister*innen zu Datenschutz und Datensicherheit

In einem Versuch, sich einen Überblick über den Status quo von Datenschutz und Datensicherheit bei österreichischen Gesundheitsdienstleister*innen zu verschaffen, wurde ein Fragebogen konzipiert. Dieser richtete sich an alle, die im Gesundheitswesen tätig sind und mit Patient*innendaten zu tun haben. Um ein möglichst breites Feld an Teilnehmenden zu erhalten, wurde der Fragebogen über verschiedene Kanäle der Standesvertretungen und Kammern versendet, mit der Bitte um zahlreiche Teilnahme.

Der Rücklauf war mit 61 vollständig ausgefüllten Fragebögen weniger umfangreich als erhofft, jedoch können auch anhand der relativ geringen absoluten Zahl an Teilnehmenden interessante Trends dargestellt werden. Betont wird aber, dass diese Ergebnisse in keiner Weise repräsentativ sind. Sie stellen nur die Aufnahme eines kleinen Ausschnitts der österreichischen Gesundheitsbranche dar.

Wenig überraschend nutzt die überwältigende Mehrheit der Befragten einen Stand-PC für die Arbeit, ein Laptop ist bei beinahe der Hälfte dieser Personen im Einsatz. Andere Endgeräte werden selten verwendet (siehe Abbildung 3). Rund 44 Prozent der Befragten gaben an, sowohl Laptop als auch Stand-PC zu verwenden. Mehr als die Hälfte dieser Geräte ist über ein LAN-Kabel mit dem Internet verbunden, mehr als jedes dritte Gerät geht per WLAN online. WLAN-Netzwerke sind anfälliger für Angriffe als ein geschlossenes LAN-Netzwerk, das auch die bevorzugte Verbindung zwischen dem Arbeitsgerät, auf dem Patient*innendaten verarbeitet werden, und der digitalen Außenwelt sein sollte.

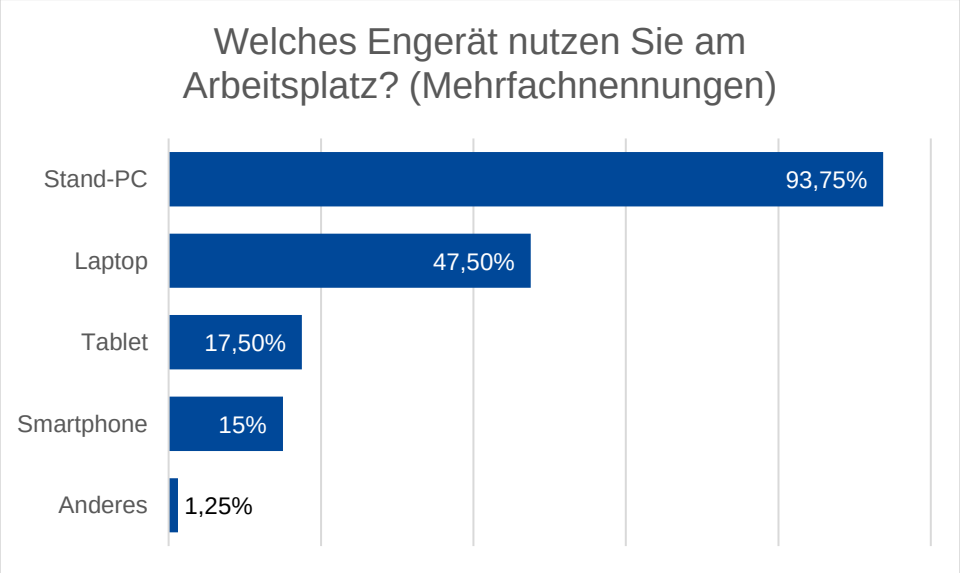

Abbildung 3: Übersicht der genutzten Endgeräte am Arbeitsplatz

Mehr als die Hälfte der Befragten gaben an, die Endgeräte am Arbeitsplatz auch für private Zwecke zu verwenden. Dies ist allerdings ein Risiko, das bestmöglich vermieden werden sollte. Denn privates Surfen ist immer auch mit weniger Sorgfalt verbunden und steuert auch andere Bereiche des Internets an. Damit ist das Risiko auch größer, eine Schadsoftware oder andere Angriffe zu erleiden, die zu einem Verlust wertvoller und hochsensibler Patient*innendaten führen können.

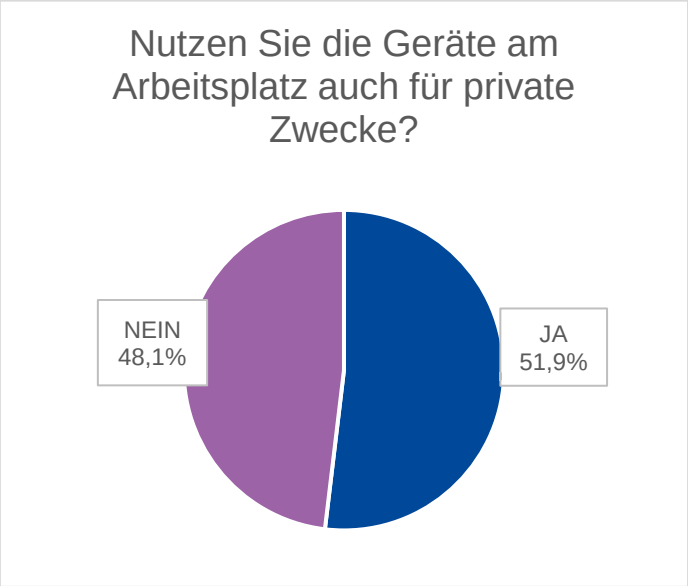

Abbildung 4: Verwendung der Endgeräte am Arbeitsplatz

Betrachtet man die grundsätzlich vorgenommenen Schutzmaßnahmen an den Geräten, zeigt sich zweierlei: Zum einen nutzen die meisten Befragten nur einen Passwortschutz, um ihre Geräte vor Fremdzugriff zu schützen – nur eine absolute Minderheit verwendet mehr als eine Authentifizierungsform (Abbildung 5). Gerade an Geräten, die zur Verarbeitung von Daten genutzt werden, sollte eine Zwei-Wege-Authentifizierung Standard sein, um das Gerät bestmöglich zu schützen.

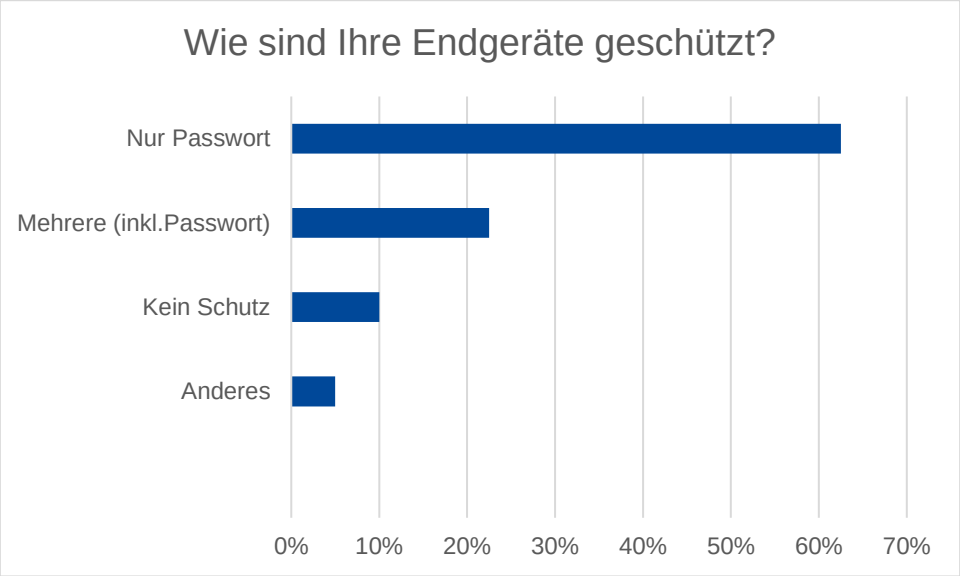

Abbildung 5: Sicherung der Endgeräte

Zum anderen zeigt sich aber auch, dass die Disziplin bei der Sicherheit der Passwörter selbst verbesserungswürdig ist. Zum einen werden die meisten Passwörter auf mehr als einem Gerät verwendet (Abbildung 6). Damit besteht das Risiko, dass ein einmal geknacktes/erbeutetes Passwort einem*einer Verbrecher*in Zugang zu mehreren Geräten erlaubt. Nur jede*r fünfte Befragte nutzt eine Passwort-Software zur Sicherung, mehr als die Hälfte der befragten Personen speichern ihre Passwörter gar nicht.

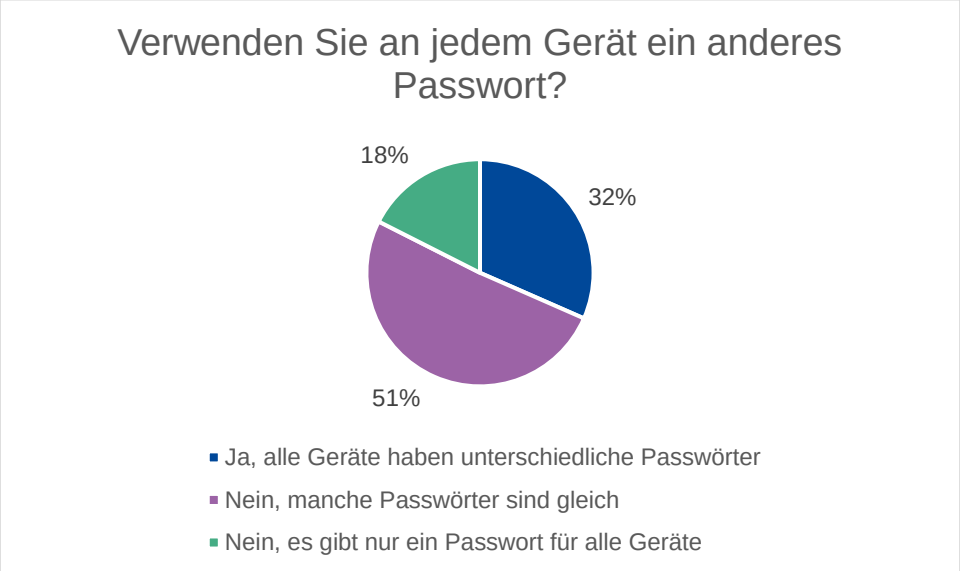

Abbildung 6: Passwortschutz: Mehrfachverwendung

Befragt nach den Cybersicherheitsmaßnahmen, die am Arbeitsplatz getroffen wurden, zeigt sich, dass sich das Gesundheitswesen in diesem Aspekt nicht allzu sehr von anderen Unternehmen unterscheidet. Die klassischen Schutzmaßnahmen (Firewall und Virenscanner) sind weit verbreitet, doch immerhin jede*r Fünfte der Befragten hat keine Firewall installiert, und jede*r

Vierte keinen Virenscanner. Während regelmäßige Updates und ein Spamschutz noch von immerhin zwei Drittel der Befragten eingesetzt werden, sieht es bei anderen Schutzmaßnahmen sehr spärlich aus. Nicht mal jede*r Zweite führt regelmäßig externe Datenbackups durch. Diese sind aber essenziell, um im Falle eines Angriffs mit einer Verschlüsselungssoftware den Betrieb aufrecht erhalten zu können. Einen sicheren E-Mail-Client – zur verschlüsselten und sicheren Kommunikation mit Patient*innen, anderen Dienstleister*innen und weiteren Adressat*innen – hat sogar nur knapp mehr als ein Drittel der Befragten (Abbildung 7).

Positiv zu bemerken ist, dass nur eine kleine Minderheit die Einrichtung von technischen Geräten und Computern selbst übernimmt. 80 Prozent geben an, die Installation durch externe Dienstleister*innen durchführen zu lassen. In einer immer komplexer werdenden digitalen Welt wird es immer wichtiger, die Einrichtung von Arbeitsgeräten Profis zu überlassen.

In der hier vorliegenden quantitativen Momentaufnahme zeigt sich ein großes Verbesserungspotenzial im Bereich der einfach zu ergreifenden Schutzmaßnahmen. Hier gibt es von professionellen Dienstleister*innen zusammengestellte Pakete, die einen umfassenden Schutz vor den unterschiedlichsten Formen von Cyberangriffen bieten. Die dafür entstehenden Kosten sollten von den Betrieben unbedingt als Investment begriffen werden. Denn Datensicherheit wird immer mehr zu einem essenziellen Bestandteil jeder Dienstleistung.

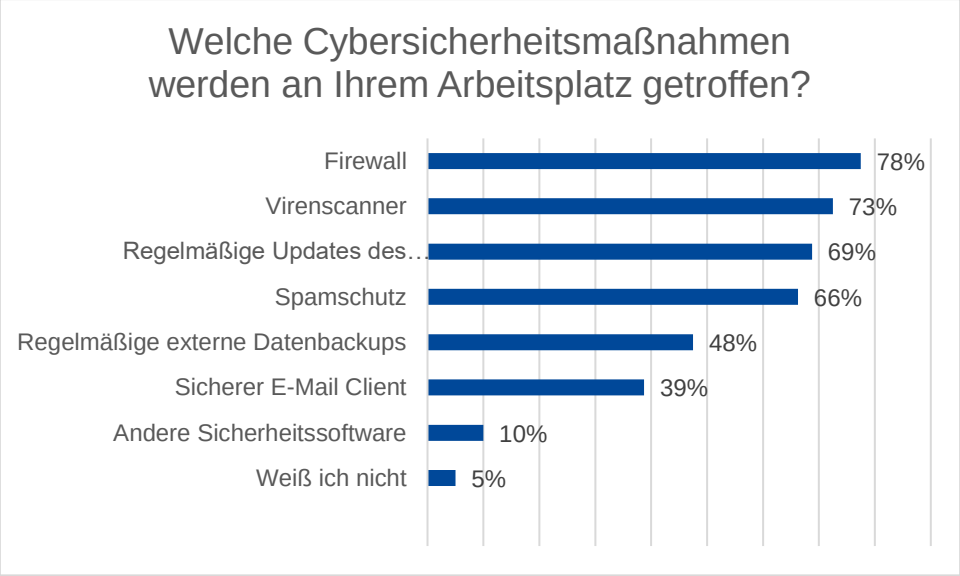

Abbildung 7: Ergriffene Cybersicherheitsmaßnahmen

Betrachtet man noch die Frage, wo Patient*innendaten gespeichert werden, zeigt sich, dass die meisten Befragten nach wie vor auf Festplattenlösungen setzen. Dies ist zwar möglicherweise der platzintensivere Weg, die Daten zu speichern, jedoch bestehen durchaus Sicherheitsvorteile gegenüber einer Cloud-Lösung (die immerhin von acht Prozent genutzt wird, siehe Abbildung 8).

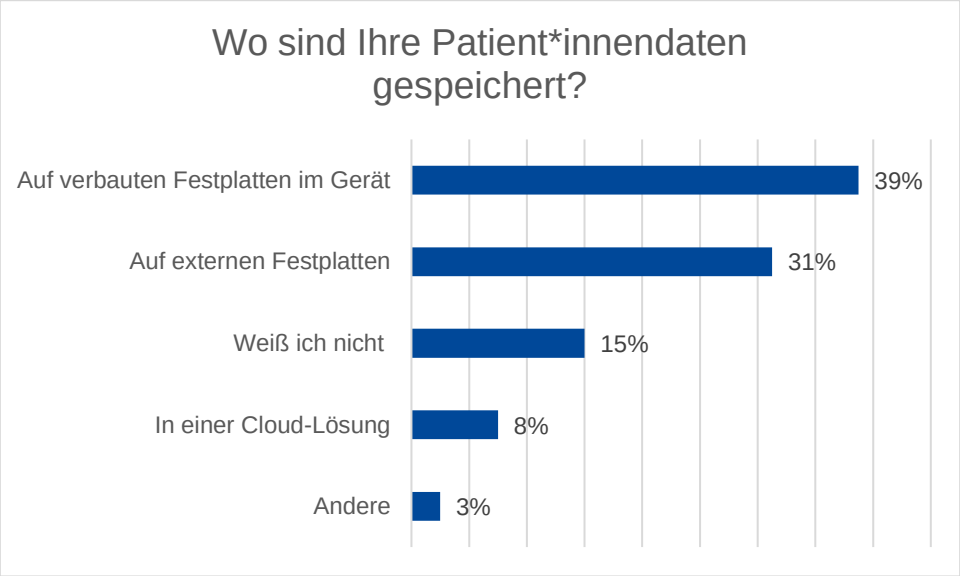

Abbildung 8: Speicherort der Patient*innendaten

In der zweiten zentralen Kategorie, dem Datenschutz, sieht die Momentaufnahme insgesamt ähnlich aus wie im Bereich Datensicherheit. Es gibt positive Anzeichen, allerdings mit viel Luft nach oben. Fast ein Viertel der befragten Unternehmen hat eine*n konkrete*n Datenschutzbeauftragte*n – diese Person ist jedoch erst ab einer gewissen Unternehmensgröße verpflichtend, die die meisten der befragten Unternehmen nicht erfüllen. Zusätzlich gibt immerhin mehr als die Hälfte der Befragten an, dass die für den Datenschutz zuständige Person auch eine entsprechende Ausbildung hat (Abbildung 9). Fast drei Viertel der Befragten wünschen sich für sich selbst oder die zuständige Person eine solche Ausbildung (Abbildung 10). Hier besteht also viel Potenzial für Kammern und Standesvertretungen, um in die Verbesserung des Datenschutzes im Gesundheitswesen zu investieren.

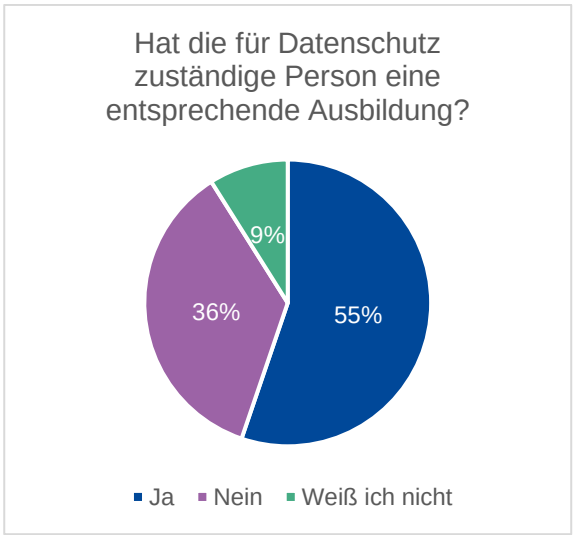

Abbildung 9: Ausbildung der für Datenschutz zuständigen Person

Abbildung 10: Wunsch nach Ausbildung im Datenschutz

Im Bereich der Richtlinien und Protokolle erkennt man, wie die DSGVO und die begleitenden Informationen zu wirken begonnen haben. 90 Prozent der Befragten geben an, eine Datenschutzrichtlinie im Unternehmen etabliert zu haben, knapp die Hälfte greift hier auf Vorlagen der Interessens- oder Standesvertretung zurück (Abbildung 11). Eine entsprechende Richtlinie ist nicht nur rechtlich erforderlich, sondern führt im Allgemeinen auch zu einem gesteigerten Problembewusstsein im Unternehmen in Bezug auf den Umgang mit Daten.

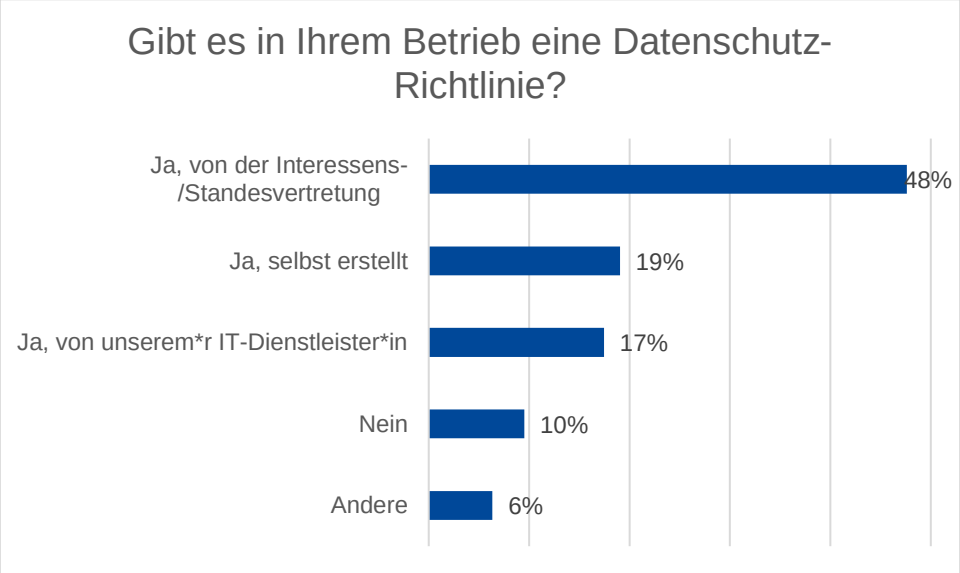

Abbildung 11: Datenschutzrichtlinie

Einheitliche Protokolle für den Umgang mit Störfällen oder Cyberattacken werden seltener implementiert. Knapp die Hälfte der großen Unternehmen (mit mehr als 10.000 Patient*innendaten) haben solche Protokolle etabliert. Unternehmen mit weniger als 10.000 Datensätzen weisen allerdings ein weit niedrigeres Level auf (Abbildung 12). Ein solches Protokoll kann jedoch im Falle eines Angriffs die interne Reaktionszeit minimieren und den Schaden geringer halten. Darüber hinaus ist mit so einem Dokument jedem*jeder Einzelnen klar, was zu tun ist, sollte ein Störfall auftreten.

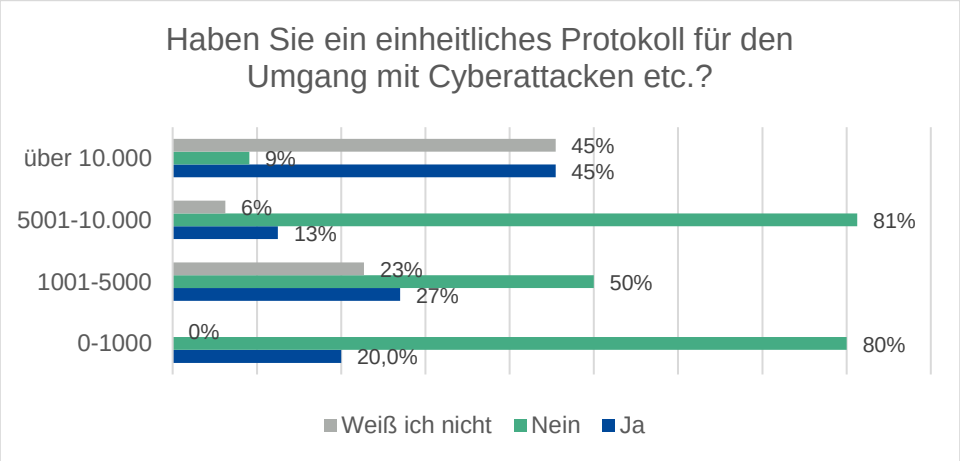

Abbildung 12: Protokoll für Cyberattacken, Störungen usw.

Abschließend wurden die Teilnehmer*innen gefragt, ob es im vergangenen Jahr zu Cybersicherheitsvorfällen an ihrem Arbeitsplatz kam. Vier Befragte (7 Prozent) meldeten einen Versuch, der jedoch durch die internen Sicherheitsmaßnahmen abgewehrt werden konnte, insgesamt neun Personen gaben an, dies nicht zu wissen. Alle Versuche wurden bei Unternehmen mit einer Datenbank von mehr als 10.000 Patient*innendaten registriert (siehe Abbildung 13). Es gab bei den versuchten Cyberangriffen jeweils einen Fall von Hacking und Phishing, die zwei weiteren Betroffenen konnten keine näheren Angaben machen. Die hier dargestellte Momentaufnahme zeigt also, dass es auch in Österreich zu Angriffsversuchen auf Gesundheitsdienstleister*innen kommt. Die befragten Betroffenen konnten diese Störversuche aber glücklicherweise abwehren.

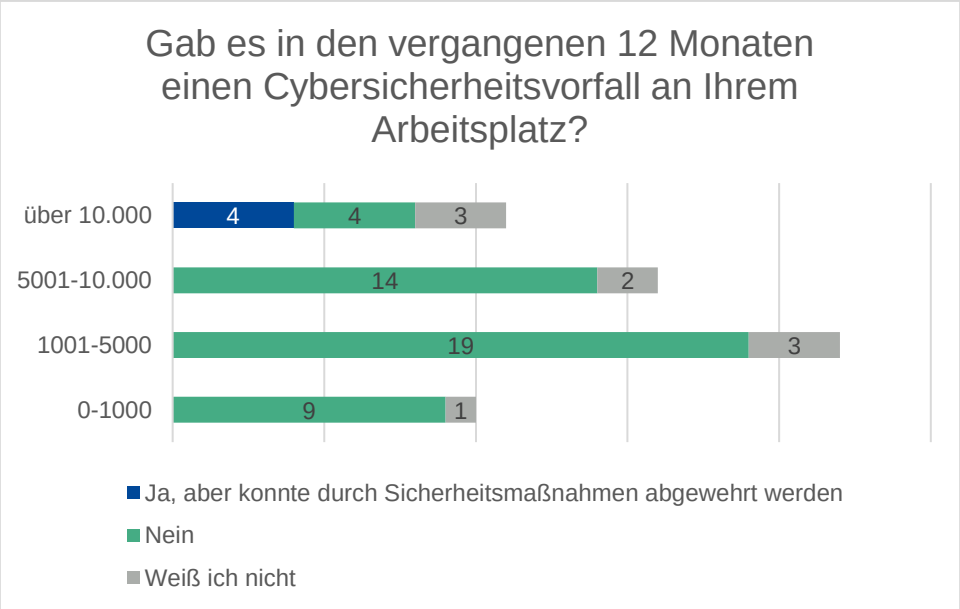

Abbildung 13: Cybersicherheitsvorfälle in den letzten 12 Monaten nach Größe der Patient*innendatenbank

Bemerkenswert positiv ist der Umgang mit diesen versuchten Angriffen: Immerhin zwei von vier Betroffenen gaben an, den Vorfall bei der Polizei angezeigt zu haben. Und alle vier meldeten den

Vorfall der Datenschutzbehörde. Dies ist ein guter Umgang mit solchen Vorfällen. Auch Angriffsversuche sollten der Polizei gemeldet werden, damit diese zielgerichtet potenzielle Opfergruppen warnen kann und über aktuelle Gefahrenlagen informiert ist. Eine Meldung bei der Datenschutzbehörde ist ebenfalls der richtige Weg, um sich und seine Daten möglichst transparent und umfassend zu schützen.

5.3. Experiment „White-Hat-Hack“ – die Ergebnisse

Die Firma Greybox IT Services (David Schwaiger, BSc) führte im Auftrag des KFV in Kooperation mit der Plattform Patientensicherheit ein externes und internes IT-Security Assessment durch. Dabei wurde mit einem*r freiwilligen medizinischen Dienstleister*in ein Security Check durchgeführt, um anhand dieses Beispiels zu zeigen, wo mögliche Schwachstellen der digitalen Sicherheit z.B. in einer durchschnittlichen Apotheke liegen.

Externes Security Assessment

Beim Externen Security Assessment wurden über das Internet erreichbare Services überprüft. Die Geschäftsführung sowie relevante IT-Dienstleister*innen waren über den Penetrationstest im Voraus informiert, um einen reibungslosen Ablauf zu gewährleisten. Die Angreifer*innen erhielten außer der Firmen-Domain keine weiteren Informationen oder Zugangsdaten.

Die Test-Attacke zeigte: Die externen Ressourcen (Webseite) des Dienstleisters weisen einen guten Schutz vor Cyberangriffen auf. Als Schwachstelle wurde allerdings der Hosting-Provider identifiziert, der in den USA ansässig ist. Über das Kontaktformular übermittelte Patient*innen-Dateien werden auf Servern auch außerhalb der EU hochgeladen und eventuell in Ländern mit abweichendem Datenschutz gespeichert. Auch wenn der Anbieter versichert, europäisches Datenschutzrecht zu befolgen, wird empfohlen, die Webseite und alle zugehörigen Services auf Servern innerhalb der EU bei einem sicheren Anbieter zu hosten.

Internes Security Assessment

Beim internen Security Assessment wurde die lokale IT-Infrastruktur des medizinischen Dienstleistungsbetriebs überprüft. Die Mitarbeiter*innen waren über die Analysen im Vorhinein informiert. Die Angreifer*innen erhielten als Ausgangssituation eine freie Netzwerkdose sowie einen Arbeitsplatz, weitere Informationen oder Zugangsdaten wurden nicht übergeben. Während der Analysen wurden sechs Schwachstellen gefunden. So war es etwa möglich, den Hauptserver des Dienstleistungsbetriebs als Administrator zu übernehmen. Mit diesen weitreichenden Zugriffsrechten konnten alle am Server gespeicherten Daten abgerufen werden. Zudem könnte ein Angreifer eigene Administrator-Benutzer anlegen, Zugangsdaten zu medizinischen Applikationen abgreifen oder alle Daten im Netzwerk verschlüsseln, um Geld zu erpressen.

Zudem wurde während der Analyse festgestellt, dass fast jedes Gerät im Netzwerk Default Zugangsdaten gesetzt hatte. Dadurch kann sich jede*r Benutzer*in, der*die die jeweiligen Standardpasswörter recherchiert hat, auf den Geräten als Administrator anmelden. Zudem wurde auf drei Systemen nicht mehr unterstützte End-Of-Life-(EOL)-Software gefunden. Da diese

Software vom Hersteller keine Updates mehr erhält, kann sie nicht mehr sicher betrieben werden und sollte daher auf eine aktuelle Version gebracht werden.

Im Netzwerk des untersuchten Dienstleistungsbetriebs sind außerdem Protokolle aktiv, die Angriffe über die Software ”Responder.py” möglich machen. Dieses Tool kann genutzt werden, um Passwörter in verschlüsselter Form (Hashes) von angemeldeten Benutzer*innen zu stehlen. Mit den abgefangenen Hashes ist es möglich, sich an anderen Computern anzumelden oder via Cracking das Klartext-Passwort wiederherzustellen. Darüber hinaus wurden neun Geräte gefunden, die unverschlüsselte Telnet-Kommunikation erlauben. Da dieses Protokoll alle Daten im Klartext übermittelt, könnten dadurch Zugangsdaten abgefangen werden. Einige Windows Computer erlauben Remote Desktop Verbindungen (RDP), haben aber Network Level Authentication (NLA) nicht aktiviert. Ohne NLA kann ein Angreifer z.B. durch Screenshots an gültige Benutzernamen kommen und anschließend versuchen, das jeweilige Passwort automatisiert zu erraten.

Device Security Assessment

Auch in diesem Überprüfungsszenario wurden die Mitarbeiter*innen vorher informiert, die Auditor*innen erhielten außer physischen Zugang zum Computer keine weiteren Informationen oder Zugangsdaten.

Der Check der Test-Hacker*innen zeigte: Mit Zugang zum Gerät wäre es für Dritte möglich, sich einen eigenen lokalen Administratoren-Benutzer anzulegen. Weiters wäre es mit diesem Zugriff auch möglich, die installierte Antivirus-Lösung komplett zu löschen, um danach Schadsoftware auf dem System auszuführen. Dadurch könnten aktive Zugangsdaten kompromittiert werden. Durch fehlende Festplattenverschlüsselung können alle gespeicherten Daten im Klartext ausgelesen werden.

Das BIOS des getesteten Computers konnte direkt als Administrator benutzt werden, da kein Passwort gesetzt wurde. Ein Angreifer kann dadurch Systemeinstellungen verändern, um z.B. von einem USB-Stick aus ein Live-Betriebssystem zu starten. Da auch das Boot-Menü für jeden Benutzer frei zugänglich ist und keinerlei Beschränkungen eingestellt wurden, kann auch hiermit ein USB-Stick gestartet werden.

Die Festplatte des PC war nicht verschlüsselt (etwa via Bitlocker). Somit konnten alle lokal darauf gespeicherten Daten ausgelesen und Systemdateien verändert werden. Dies ist nötig, um im nächsten Schritt ein CMD-Befehlsterminal mit Systemrechten am Windows-Anmeldebildschirm zu öffnen. Über dieses privilegierte Terminal kann ein neuer Benutzer erstellt und der Administratoren-Gruppe hinzugefügt werden. Dieser Benutzer kann nun Programme installieren und ausführen, alle lokalen Daten herunterladen oder den Computer mit Ransomware verschlüsseln.

Auch kann auf diese Weise die Antiviren-Software gelöscht werden. In Folge kann ein Angreifer eigene Malware auf dem System ausführen und so an gültige Zugangsdaten gelangen. Zur Behebung dieses Problems sollte das BIOS aller lokalen Computer mit einem starken Passwort geschützt werden, zudem sollte das Boot-Menü für normale Benutzer auf die Windows-Partition

eingeschränkt werden. Eine Full Disk Encryption (Festplattenverschlüsselung) sollte etwa mittels Bitlocker auf allen Geräten aktiviert werden.

Phishing-Kampagne

Im Zeitraum einer Woche wurden 15 Phishing-E-Mails mit unterschiedlichen Dateianhängen verschickt. Dabei wurden zehn E-Mails über das Kontaktformular auf der Homepage versendet, fünf wurden direkt an bekannte E-Mail-Adressen versendet. Hierbei wurde zielgerichtet versucht, etwa an Zugangsdaten zur Webseite zu kommen. Ein vielversprechender Angriff mit gefälschter Login-Seite scheiterte an einem Form-Fehler (Anrede per Sie, Personen sind per Du). Kein schädliches Dokument wurde zur Ausführung gebracht, und keine Zugangsdaten wurden über die gefälschten Login-Webseiten übermittelt. Die Mitarbeiter*innen scheinen hohe Aufmerksamkeit in Bezug auf Phishing-E-Mails zu zeigen. Dies liegt auch an der Schulung durch die Leitung der Apotheke, die ihre Mitarbeiter*innen in dieser Hinsicht brieft. Das installierte Antivirenprogramm würde für den Fall, dass doch einmal ein schädliches Dokument ausgeführt wird, dieses mit hoher Wahrscheinlichkeit unschädlich machen.

WIFI Security Assessment

Die Auditor*innen konnten in Reichweite eines WIFI Hotspots arbeiten und erhielten die SSID (den Namen) des Netzwerks und für den Greybox-Teil gültige Zugangsdaten. Die Fachmeinung der Test-Hacker*innen: Aufgrund der Stärke des eingesetzten Passwortes ist es sehr unwahrscheinlich, dass sich jemand unerlaubt Zugriff auf das interne WLAN-Netzwerk verschaffen kann.

Physical Security Assessment

Während der physischen Begehung der Räumlichkeiten versuchten die als Kund*innen getarnten Test-Hacker*innen, ein Netzwerkgerät zu installieren bzw. einen Mitarbeiter zum Anstecken eines speziellen USB-Sticks zu überreden. Dabei war die Geschäftsführung über den geplanten Test im Voraus informiert, die Mitarbeiter*innen allerdings nicht. Die Auditor*innen erhielten außer der Adresse keine weiteren Informationen über den*die Gesundheitsdienstleister*in.

Aufgrund der baulichen Bedingungen innerhalb des Geschäftsraums war es möglich, ein spezielles Gerät für LAN-Netzwerk-Angriffe (Shark Jack) an eine Ethernet-Netzwerkdose anzuschließen und einen Scan durchzuführen. Auch wurde ein Mitarbeiter während eines Verkaufsgesprächs gebeten, den mitgebrachten USB-Stick (vorgeblich mit Informationen zu Medikamenten der Mutter) am Computer anzustecken und die darauf befindliche Datei zu öffnen. Dies wurde vom Mitarbeiter abgelehnt, er verwies auf eine erforderliche Zustellung per E-Mail.

Bei Erfolg hätte der USB-Stick automatisch bestimmte Befehle auf dem Computer ausgeführt und die Ergebnisse per E-Mail an Greybox übermittelt.

Im Nachgespräch wurde darauf hingewiesen, dass die Testperson mindestens einer Mitarbeiterin verdächtig vorkam. Es herrschte generell hohe Aufmerksamkeit gegenüber Kund*innen in den Geschäftsräumen.

Fazit

Das Fazit der IT-Fachleute nach Durchführung des Experiments: Der allgemeine Sicherheitsstandard im überprüften Gesundheitsdienstleistungsbetrieb ist als sehr hoch anzusehen. Die gefundenen Schwachstellen können leicht behoben werden, somit kann die Sicherheit weiter erhöht werden.

Dennoch zeigt auch der hier dargestellte exemplarische Fall deutlich, dass selbst in einem gut geschützten System Schwachstellen gefunden und von krimineller Energie ausgenutzt werden können. Wie in diesem konkreten Fall gezeigt, ist eine regelmäßige Ausbildung der Mitarbeiter*innen zum Thema Datensicherheit immens wichtig. Das Bewusstsein, mit welch sensiblen Daten umgegangen wird, ist in der konkret untersuchten Branche allerdings bereits stark vorhanden.

6. Conclusio

Das Sammeln von Daten ist aus der heutigen Welt nicht mehr wegzudenken. In Österreich bestand bereits vor der Einführung der Datenschutz-Grundverordnung (DSGVO) ein hohes Restriktionsniveau. Dennoch gab es nach Expert*innenmeinung eine intensive Auseinandersetzung mit den neuen Regelungen. Die Sicherheit von Patient*innendaten liegt in Österreich allgemein auf einem sehr guten Niveau, dennoch gibt es Lücken, die von Kriminellen ausgenutzt werden können. Aus den Zahlen des Bundeskriminalamtes geht deutlich hervor, dass es sich bei Cyberkriminalität um ein stark wachsendes Problem handelt (siehe Kapitel 4). Gesundheitsdaten sind aufgrund ihrer Einzigartigkeit und ihrer Verbundenheit mit der jeweiligen Person, der sie zugeschrieben sind, besonders vulnerabel, das macht sie aber auch besonders wertvoll. Daher ist ein entsprechendes Maß an Professionalität in puncto Datenschutz und Datensicherheit notwendig. Es handelt sich dabei um einen eigenen IT-Fachbereich, bei dem Alltagswissen oder Interesse an der Thematik allein meist nicht ausreicht.

Von besonderer Relevanz ist hierbei die Verschlüsselung der Daten. In der Kommunikation zwischen Dienstleister*innen oder mit Krankenkassen ist es notwendig, die Verschlüsselung von Daten standardisiert durchzuführen. In Sachen Sicherheit ist dabei noch Luft nach oben vorhanden, so der Tenor der Expert*innen (siehe Kapitel 3, 4 und 5). Diese Verschlüsselung sollte allerdings nicht nur in der Kommunikation zwischen verschiedenen Parteien des Gesundheitswesens gegeben sein, Patient*innendaten sollten ausschließlich in verschlüsselter Form gespeichert werden, um es potenziellen Eindringlingen so schwer wie möglich zu machen, an diese heranzukommen. Aktuell ist ein einfacher Passwortschutz üblich, wobei festzustellen ist, dass teilweise dasselbe Passwort für mehrere Geräte verwendet wird. Hier wäre, insbesondere wenn auf einem Gerät Patient*innendaten verarbeitet oder gespeichert werden, ein mehrstufiges Authentifizierungsverfahren empfehlenswert. Besonders der Einsatz vernetzter Geräte, die Datenspeicherung in Cloud-Diensten und der drahtlose Datentransfer spielen dabei eine wichtige Rolle, da diese viele potenzielle Schwach- und somit Angriffsstellen aufweisen.

Im Falle von Patient*innendaten kann ein Ransomware-Angriff nicht nur teuer werden, sondern sogar auch das Leben von Patient*innen bedrohen. Werden bei einem solchen die Daten von Angreifer*innen verschlüsselt und kann kein Zugriff auf die Krankengeschichte mehr erfolgen, stellt dies eine erhebliche Gefahr für Leib und Leben dar. Dies gilt im Speziellen für vulnerable Gruppen, die etwa in ihrer Kommunikationsfähigkeit eingeschränkt sind. Sollte es also zu einem erfolgreichen Ransomware-Angriff kommen, muss der Betrieb innerhalb kürzester Zeit in der Lage sein, die Daten wieder zu restaurieren. Ein funktionierendes, effektives Backup- und Recovery Konzept ist daher essenziell. So kann der Worst Case – der längerfristige Ausfall der Systeme und der Verlust der Daten – verhindert werden. Die Absicherung der Infrastruktur ist äußerst komplex und sollte mittels Partnerunternehmen aus der IT-Sicherheitsbranche erfolgen, um möglichst umfassende Lösungen zu finden. Einheitliche Protokolle für den Umgang mit Störfällen sind essenziell, um im Fall des Falles schnell und systematisch vorgehen zu können.

Der Faktor Mensch spielt im Bereich der Sicherheit von Patient*innendaten eine entscheidende Rolle. Die fachliche Kenntnis von Risiken der Datenverarbeitung, vor allem das spezifische Know-

how im Umgang mit sensiblen Daten wie diesen, ist essenziell für die Gewährleistung erforderlicher Sicherheit. Wie auch das KFV-Experiment (siehe Kapitel 5.3) eindrucksvoll zeigt, ist die persönliche Aufmerksamkeit der Mitarbeiter*innen ein Faktor, der über Gelingen oder Misslingen eines Angriffes bestimmt. Wenn die Mitarbeiter*innen regelmäßig hinsichtlich der Bedrohungsszenarien Phishing oder Ransomware sowie in Sachen Datensicherheit geschult werden, wird ein wesentliches Einfallstor für Bedrohungen geschlossen.

Eine spezielle Absicherung der Arbeitsplätze durch eingebaute Schutzmechanismen ist dennoch empfehlenswert. Vor allem im Gesundheitsbereich ist die Arbeitsbelastung tendenziell hoch, und unter solchen Voraussetzungen passieren Fehler besonders leicht. Ein zusätzliches Sicherheitsnetz kann hier hilfreich sein. Auch die private Nutzung unternehmenseigener Geräte eröffnet Kriminellen potenzielle Zugangsmöglichkeiten. In diesem Fall gewinnen zusätzliche Schutzmaßnahmen und Vorkehrungen noch einmal an Relevanz.

Ein beständiger Informationsfluss vonseiten der zuständigen Stellen (Ärztekammer, Apothekerkammer etc.) in Form von Leitfäden zum Umgang mit Daten und der Sicherheit innerhalb der Unternehmen ist jedenfalls empfehlenswert. Sinnvoll ist auch der Einsatz eines Systems unterschiedlicher Berechtigungsstufen für Mitarbeitende, so dass jede Person nur jene Zugriffsrechte hat, die sie unbedingt benötigt. Auf diese Weise wird das Risiko, dass ungeschultes Personal mit Datensätzen hantiert, die für die eigene Arbeit nicht notwendig sind, minimiert.

Die Verschränkung von Gesundheitsdaten für wissenschaftliche Zwecke ist wünschenswert, doch nur, wenn dabei die persönlichen Daten der*des Einzelnen geschützt bleiben. Derartige Datensammlungen müssen sich am Konzept Privacy by Design orientieren und so Rückschlüsse auf die Person hinter den anonymisierten Daten verhindern. Dabei ist eine zentrale Stelle, die diese Daten sicher speichert, sinnvoll. Viele kleine Dienstleister*innen, die diese Daten an unterschiedliche Stellen kommunizieren, erhöhen das Einfallrisiko für Bedrohungen.

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

Argaw, S., Bempong, N.-E., Eshaya-Chauvin, B. & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Medical Informatics and Decision Making*.

Argaw, S., Troncoso-Pastoriza, J., Lacey, D., Florin, M.-V., Calcavecchia, D., Burleson, W., . . . Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*.

Berger, R. (2017). *Krankenhausstudie.* München.

Bundeskriminalamt. (2020). *Cybercrime Report 2019.* Wien: Bundesministerium für Inneres. Abgerufen am 11. November 2020 von https://bundeskriminalamt.at/306/files/Cybercrime_2019.pdf

Center for Internet Security (2021). *Data Breaches: In the Healthcare Sector*. Abgerufen am 21. Oktober 2021 von cisecurity.org: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/

Davis, J. (2021). *UHS Ransomware Attack Cost $67M in Lost Revenue, Recovery Efforts*. Abgerufen am 12. Oktober 2021 von Health IT Security: https://healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue

Der Spiegel (2017). *Cyberattacke trifft Ziele weltweit*. Abgerufen am 21. Oktober 2021 von spiegel.de: https://www.spiegel.de/netzwelt/web/grossbritannien-cyber-attacke-auf-krankenhaeuser-sorgt-fuer-aufregung-a-1147453.html

Forgó, N. (20. Juli 2021). Sicherheit von Patient*innendaten. (G. Plattner, Interviewer)

Gesamtverband der Deutschen Versicherungswirtschaft (2018). *Kostbare Beute Patientendaten*. Abgerufen am 21. Oktober 2021 von gdv.de: https://www.gdv.de/de/themen/news/kostbare-beute-patientendaten-31284

Gordon, W., Wright, A., Aiyagari, R., Corbo, L., Glynn, R., Kadakia, J., . . . Landman, A. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open* (2(3)).

Gordon, W., Wright, A., Aiyagari, R., Corbo, L., Glynn, R., Kadakia, J., . . . Scheib, P. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*.

Habl, C. & Degelsegger-Márquez, A. (21. September 2021). Sicherheit von Patient*innendaten. (G. Plattner & A. Fassl, Interviewer)

Jalali, M. & Kaiser, J. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research.

Jalali, M., Razak, S., Gordon, W., Perakslis, E. & Madnick, S. (2019). Health Care and Cybersecurity: Bibliometric Analysis of the Literature. *Journal of Medical Internet Research*.

Jalali, M., Russell, B., Razak, S. & Gordon, W. (2019). EARS to cyber incidents in health care. *Journal of the American Medical Informatics Association*, S. 81-90.

Jalali, S., Bruckes, M., Westmattelmann, D. & Schewe, G. (2020). Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research*.

Kelly, J., Campbell, K., Gong, E. & Scuffham, P. (2020). The Internet of Things: Impact and Implications for Health Care Delivery. *Journal of Medical Internet Research*.

Kneip, F. (2020). *IT-Sicherheit im Krankenhaus – Herausforderungen meistern*. Abgerufen am 11. Oktober 2021 von SoSafe.de: https://sosafe.de/blog/it-sicherheit-im-krankenhaus/

Kunz, T., Lange, B. & Selzer, A. (2020). Datenschutz und Datensicherheit in Digital Public Health. *Bundesgesundheitsblatt*.

Lang, E., Pfandlsteiner, E.-M., Satzinger, G., Scharinger, R., Schmeissl, B. & Worel, T. (2019). *Schutz sensibler Daten. Positionen der Gesundheitssektionen VIII und IX des BMASGK.* Wien: Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz (BMASGK).

Lenz, P. & Masicek, T. (07. Oktober 2021). Sicherheit von Patient*innendaten. (G. Plattner & A. Fassl, Interviewer)

Spinazze, P., Aardoom, J., Chavannes, N. & Kasteleyn, M. (2021). The Computer Will See You Now: Overcoming Barriers to Adoption of Computer-Assisted History Taking (CAHT) in Primary Care. *Journal of Medical Internet Research*.

Umizeyemungu, S., Poba-Nzaou, P. & Cantinotti, M. (2019). European Hospitals' Transition Toward Fully Electronic-Based Systems: Do Information Technology Security and Privacy Practices Follow? *JMIR Medical Informatics*.

Widup, S., Spitler, M., Hylender, D. & Bassett, G. (2018). *2018 Verizon Data Breach Investigations Report.*

Williams, C., Chaturvedi, R. & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*.

KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien
T +43-(0)5 77 0 77-DW oder -0
F +43-(0)5 77 0 77-1186
E-Mail kfv@kfv.at
www.kfv.at

Medieninhaber und Herausgeber: Kuratorium für Verkehrssicherheit
Verlagsort: Wien
Herstellung: Eigendruck
Redaktion: Patricia Jeßner, BA
Grafik: eigene Darstellung
Titelbild: Pixabay/DarkoStojanovic

SAFETY FIRST!