Angemessene Paranoia

© beebright / Fotolia

Noch kann nicht behauptet werden, dass der österreichische Gesundheitssektor ausreichend gegen Computerkriminalität geschützt ist. Angesichts der potenziellen Gefahren für die Patienten und ihre Daten drängt die Zeit.

Alexandra Keller

Ende März 2019 ging Wikipedia für einen Tag offline. Aus Protest gegen die EU-Urheberrechtsreform war die deutschsprachige Version der Online-Enzyklopädie für 24 Stunden komplett stillgelegt worden und die satirische österreichische Online-Tageszeitung *Die Tagespresse* bedachte diesen Tag mit einem Bericht. „Wikipedia heute offline: Tausende Ärzte können keine Diagnose stellen" wurde die kurze Satire betitelt, in der nicht nur die Hilflosigkeit der Mediziner ohne Internet aufs Korn genommen, sondern auch ein Kern Wahrheit getroffen wurde. In zahlreichen Bereichen hat sich die Medizin längst von ihren analogen Wurzeln verabschiedet und Schritt für Schritt in die Abhängigkeit „der IT" begeben.

Ärztezimmer und Ordinationen werden immer weniger von Bücherrücken im typischen Dunkelblau, Hellblau und Weiß beherrscht. Stehen diese Lehrbücher doch noch in den Regalen, so fangen sie dort eher Staub, als dass sie für die Beantwortung diagnostischer Fragen zu Rate gezogen würden. Nachschlagen in Fachbüchern darf oftmals durch „Nachklicken" im Internet ersetzt werden. Darum trifft die Satire einen Kern.

Dass der Gesundheitssektor auf allen Ebenen von einer digitalen Megawelle erfasst wurde, ist nicht neu. „Computer werden in naher Zukunft 80 Prozent der Funktionen erfüllen, die heute Ärzte erbringen", ist etwa der Schweizer Zukunftsforscher Georges T. Roos überzeugt. Während die Hintergründe für seine These zwingend zu einer grundlegenden Debatte über das neue ärztliche Selbstverständnis führen, werden allerorts die IT-Systeme aufgemotzt, um bei der Entwicklung mithalten zu können.

Nicht ausreichend

„Wenn ein Krankenhaus ein neues Krankenhaus-Informationssystem installiert, dann wird viel Zeit und Energie für Informationen darüber verwendet, was das System alles kann. Meiner Erfahrung nach wird aber nicht ausreichend Zeit und Energie verwendet, um die Sicherheit der Systeme zu diskutieren", stellt Cornelius Granig fest. Granig ist Unternehmensberater und Cybersicherheitsexperte, er steht der Ärztekammer in diesen Fragen zur Seite und deutet mit seinem Anfang April 2019 erschienenen Buch *Darknet – Die Welt im Schatten der Computerkriminalität* mahnend auf arg kränkelnde Tatsachen. „Die Sicherheit ist stark steigerbar", sagt Granig zum Status quo der Systeme im heimischen Gesundheitssektor.

Die Diplomatie seiner Worte entbehrt nicht einer gewissen Dramatik. Und dramatisch ist es auch, was die digitalen Welten im Gesundheitswesen für die Patienten im negativen Fall bedeuten können. „Wir haben Telemedizin, elektronische Patientenakten, Fitnesstracker, Pflegeroboter, digitale Unterstützung bei Operationen und zahlreiche Geräte, die in den Bereich Internet der Dinge fallen", umreißt Granig im Gespräch mit der *ÖKZ* grob das digitale Gesundheitsuniversum, in dem sich auch Kriminelle tummeln. Mit stark steigender Tendenz beziehungsweise Frequenz.

Am 2. Mai 2019 erst veröffentlichte das österreichische Innenministerium die *Polizeiliche Kriminalstatistik 2018*, und diese weist eine starke Zunahme der Computerkriminalität aus. Gegenüber dem Vorjahr waren die Fälle von Cybercrime um 16,8 Prozent auf fast 20.000 in die Höhe geschnellt. Weil viele Betroffene die Angriffe nicht melden oder keine Anzeige erstatten, ist die Dunkelziffer allerdings sehr hoch. „Datenlecks im Gesundheitsbereich sind besonders heikel. Der Gesundheitsbereich ist ein Anziehungspunkt für viele Straftäter, da hier äußerst sensible, personenbezogene Daten verarbeitet werden, die für viele Delikte genutzt werden können. Die Absicherung dieser Systeme ist sehr wichtig", so Granig.

Wird beispielsweise ein über Bluetooth ansteuerbarer Herzschrittmacher oder eine Insulinpumpe gehackt, hat der Hacker die Möglichkeit, den Betroffenen krank zu machen oder gar zu töten. Um die Gefahren aufzuzeigen, darf nicht tiefgestapelt werden. Ohne angemessene Sicherheitsmaßnahmen können Spitäler lahmgelegt, Patientendaten gestohlen und ganze Systeme ins Wanken gebracht werden.

IT-Experte und Buchautor Cornelius Granig: „Datenlecks im Gesundheitsbereich sind besonders heikel."

Verwundbarkeit des Netzes

Cybersicherheit ist das Schlüsselwort, das sich wie ein roter Faden durch Granigs Buch zieht und auch die Datenlecks im österreichischen Gesundheitssektor umspannt. 2009 wurde beispielsweise das Netzwerk der Kärntner Landeskrankenhäuser mit einem Computerwurm infiziert, der rund 3000 Krankenhaus-PCs lahmlegte und damit auch den Krankenhausbetrieb. 2010 wurde die Website des Tiroler Krankenanstaltenverbundes manipuliert und mit einer Kinderpornografie-Seite verlinkt, was nicht sicherheitskritisch klingt, wohl aber die Verwundbarkeit des Netzes aufzeigt. 2011 wurde die Tiroler Gebietskrankenkasse (TGKK) beziehungsweise ihre Versicherten Opfer eines veritablen Angriffs. Den Hacktivisten von Anonymous Austria war es gelungen, an über 600.000 Datensätze der TGKK zu kommen. Die Internet-Aktivisten gaben an, zufällig über die Daten gestolpert zu sein, der TGKK-Obmann sprach von einer „kriminellen Geschichte", Anzeige gegen Unbekannt wurde erstattet und in einer ersten Reaktion war ausgeschlossen worden, dass die doppelte Firewall gehackt wurde. „Wie in vielen ähnlich gelagerten Fällen wurde von der TGKK sofort betont, wie gut die Absicherung nach außen sei. Offenbar denkt man häufig nicht daran, dass die meisten Datendiebstähle intern passieren oder zumindest in Zusammenarbeit zwischen externen Angreifern und internen Mittätern", lenkt der Autor den Blick weg von stolz präsentierten Firewalls ins Innere der Gemäuer, wo kriminelle Energie oder das IT-Know-how nicht riesig sein müssen, um immensen Schaden anrichten zu können. „Heute kann man mit einem USB-Stick in Windeseile tausende Daten mitnehmen. Computerkriminalität ist sehr einfach geworden", weiß Granig. Ein Arbeitscomputer im Netz, ein USB-Eingang, Frust wegen wem oder was auch immer, ein Quäntchen Rachedurst und ein USB-Stick um 17,99 Euro. Mehr ist nicht nötig.

„Die Zahl der Menschen, die Daten kopieren dürfen, muss sehr klein gehalten werden. Man muss mitloggen, wer kopiert und

Es ist wichtig, Angriffe auf die Cybersicherheit öffentlich zu machen.

man muss laufend Background-Checks machen“, forciert der Experte eine Art angemessene Paranoia und hält fest: „Man muss einfach vorsichtig sein und mehr Respekt vor dieser Bedrohung haben.“

Als im Herbst 2013 der Hauptverband der Sozialversicherungsträger nach anfänglichem Zögern und einem eigentümlichen Dementi-Reigen ein Datenleck in der Zentralen Partnerverwaltung (ZPV) eingestehen musste, wurde rasch davon ausgegangen, dass ein interner Mitarbeiter die Daten an Anonymous Austria weitergegeben hatte. „Beim Hauptverband reden wir über die größte und zentralste Datenbank der österreichischen Gesundheitswelt. Die ZPV hat mehr als 15 Millionen personenbezogene Daten gespeichert“, sagt Granig, der auch die zahlreichen potenziell gefährlichen Designmängel im Zusammenhang mit der Elektronischen Gesundheitsakte (ELGA) kennt, die er in Zusammenarbeit mit der Wiener Ärztekammer in einer 2016 veröffentlichten Studie aufgezählt hat und die – wie er schreibt – bisher noch nicht behoben wurden. Von der *ÖKZ* mit der Mängelliste konfrontiert, klärt die ELGA GmbH auf, dass einzelne Forderungen teilweise bereits umgesetzt wurden und andere aufgrund der fehlenden gesetzlichen Grundlagen nicht umgesetzt werden können. Zu der, auch im Buch veröffentlichten Forderung nach „Einführung einer verpflichtenden separaten Authentifizierung beim Einstieg in ELGA, damit beispielsweise in Krankenhäusern die ELGA-Anmeldung nicht mit der Anmeldung zum Krankenhaus-Informationssystem verknüpft wird (kein Single-Login)“, wird von der ELGA GmbH beispielsweise festgehalten: „Das wäre eine Usability-Hürde, die keinen oder kaum einen sicherheitstechnischen Mehrwert aufweisen würde. Genau dort werden sämtliche hausintern erfassten oder hausextern angeforderten oder vom Patienten mitgebrachten Daten verwaltet und benötigt. Die Daten, die über ELGA-Services dort für die in Behandlung stehenden Patientinnen benötigt werden, entsprechen von der erforderlichen Sicherheitsstufe exakt denselben Kriterien.“ Jedenfalls Recht behält Granig aber, wenn er sagt: „Es wäre ein absoluter Supergau, wenn das ELGA-System gehackt wird oder jemand auch nur Teile der Daten aus dem System bekommt.“

Auch die Zurückhaltung der Institutionen, über bereits erfolgte Angriffe zu sprechen, taucht die Cybersicherheitslage des österreichischen Gesundheitssektors in einen eigentümlichen Nebel. Um Welten transparenter wird in den USA mit dem Problem umgegangen. Dort gibt es eine Melde- und Veröffentlichungspflicht für Angriffe auf Krankenhäuser, die mehr als 500 Patienten betreffen. Das „Breach Portal“ des US-amerikanischen Gesundheitsministeriums kann jederzeit und von jedem eingesehen werden. Für April 2019 werden dort beispielsweise 37 Fälle aufgelistet, die der Behörde gemeldet wurden und von ihr untersucht werden. Mit 197.661 betroffenen Patienten war der Hackerangriff auf das Netzwerk der kalifornischen Centrelake Medical Group Inc. der größte im April dieses Jahres und es ist gut möglich, dass potenzielle Patienten diese Einrichtung meiden, nachdem sie die Website durchforstet haben. Zwischen 2010 und 2016 waren laut einer in *Darknet* zitierten norwegischen Studie 171 Millionen US-Amerikaner von Gesundheits-Datenlecks betroffen, was rund 54 Prozent der Gesamtbevölkerung entspricht. „Es ist sehr wichtig, diese Informationen öffentlich zu machen. Denn dadurch können einerseits Patienten die Vertrauenswürdigkeit von Krankenhäusern besser beurteilen, und andererseits ist es für die Betreiber ein Ansporn, die Sicherheitsvorkehrungen zu intensivieren“, sagt der Autor, der ein ähnliches System auch in Österreich für „andenkenswert“ hält und grundsätzlich Folgendes festhält: „Meiner Meinung nach müssen die Krankenanstalten massive Investitionen tätigen, um zeitgemäßen Schutz zu erreichen.“

Unheimliche Dimensionen

Der Investitionsstau scheint enorm zu sein und allein das Fehlen diesbezüglich strenger Vorschriften – die Finanzbranche lebt ein solches Modell mit der Finanzmarktaufsicht als Regulator längst vor – stellt die Verantwortlichen vor enorme Herausforderungen. Und ein bisschen auch an den Pranger, weil die Folgen von Datenlecks unheimliche Dimensionen für die Betroffenen annehmen können.

Ende 2018 begann in Litauen beispielsweise ein Gerichtsprozess gegen Beschuldigte aus dem Umfeld einer Schönheitsklinik. Die Angeklagten hatten 25.000 Fotos und Gesundheitsinformationen aus der von internationalen Patienten frequentierten Klinik gestohlen und im Netz veröffentlicht. „Die Gangster verlangten zwischen 50 und 2000 britische Pfund, die in Bitcoin bezahlt werden sollten – je nachdem, wie sensibel die Fotos waren –, um diese wieder vom Netz zu nehmen“, so der Autor, der den österreichischen Präsidentschaftswahlkampf 2016 an den Beginn des *Darknet*-Kapitels über die „Kranken Daten“ stellt. Damals wurde nicht nur der Gesundheitszustand des späteren Bundespräsidenten Alexander van der Bellen in Frage gestellt, auch sein Herausforderer Norbert Hofer geriet in Erklärungsnot, nachdem den Medien infolge eines Datenlecks in der Pensionsversicherungsanstalt ein abgelehnter Antrag Hofers auf die Gewährung einer Invaliditätspension zugespielt worden war. Dazu hält Cornelius Granig fest: „Dieser Fall illustriert sehr gut, welch wichtige Rolle Datenlecks aus dem Gesundheitsbereich gerade in heiklen beruflichen Situationen spielen können.“ ::

Cornelius Granig: Darknet. Die Welt im Schatten der Computerkriminalität. Kremayr & Scheriau, Wien 2019. ISBN: 978-3-218-01157-0

Alexandra Keller
Journalistin, Innsbruck
alexandra.keller@chello.at