MEDIENDIENST DER ÖSTERREICHISCHEN ÄRZTEKAMMER

Inhaber, Herausgeber,
Hersteller und Redaktion:
Österreichische Ärztekammer
Öffentlichkeitsarbeit
A-1010 Wien, Weihburggasse 10-12
Telefon 01/51406–3312 DW
pressestelle@aerztekammer.at

PRESSEKONFERENZ

Thema:

Cyberkriminalität: Wie sicher ist der Gesundheitssektor?

Teilnehmer:

a.o. Univ.-Prof. Dr. Thomas Szekeres
Präsident der Österreichischen Ärztekammer

Dr. Philipp Amann
Leiter der Strategieabteilung des European Cybercrime Centre (EC3) von *Europol*

Dr. Cornelius Granig
Leiter des Bereichs Cyber Security und Krisenmanagement beim Beratungsunternehmen Grant Thornton Austria

Zeit:

Donnerstag, 27. August 2020, 9.00 Uhr

Ort:

Österreichische Ärztekammer

Weihburggasse 10-12

1010 Wien

„Brandbeschleuniger“ für Cyberkriminalität

Die COVID-19-Pandemie hat sämtliche Bereiche des alltäglichen Lebens vor ganz neue Herausforderungen gestellt, darunter auch den Kampf gegen Kriminalität. In Zeiten des „Social Distancing“, Home Office und Telearbeit rückten der Gesundheitssektor und die wertvollen Daten, die er produziert, in den Fokus von Kriminellen. Menschen werden zunehmend mit gestohlenen Gesundheitsdaten erpresst. Und Cyberangriffe können jeden treffen: Krankenhäuser, Labors, niedergelassene Ärzte. Ziel ist es, das Bewusstsein für Sicherheitslücken zu stärken, Mitarbeiter zu schulen und Notfallpläne zu erstellen.

Statement a.o. Univ.Prof. Dr. Szekeres

Nie zuvor in unserer Geschichte hat die Menschheit so viele Daten produziert. Das beginnt bei den sozialen Medien, in denen jeder seine Gedankengänge einem Millionenpublikum präsentieren kann, und geht bis zum Trend der Selbstvermessung via Smartwatches, die schon beinahe jeden Lebensbereich überwachen und die Ergebnisse mitdokumentieren. Aus dieser Masse an Daten stechen die Gesundheitsdaten besonders heraus. Diese sehr persönlichen und besonders sensiblen Daten sind durch diese Eigenschaften von unschätzbarem Wert. Aktuell können wir das etwa an der aktuellen Pandemiesituation feststellen. Big Data, also die Auswertung von riesigen Datenmengen, hat das Potenzial, die Suche nach einem Medikament oder einem Impfstoff gegen COVID-19 erheblich zu beschleunigen. Eine internationale Verknüpfung von Gesundheits- und Medikamentendaten kann ein wichtiger Schlüssel sein, um der vorherrschenden Pandemie ein Ende zu setzen.

Dieser unfassbar große Wert macht Gesundheitsdaten aber auch besonders begehrt bei Cyberkriminellen. Entsprechend hoch ist hier auch das Thema Datenschutz zu gewichten. Das betrifft aus Ärztesicht alle Einrichtungen, in denen etwa Patienten- und Medikamentendaten erzeugt und verarbeitet werden, seien es jetzt die Arztordination oder ein Krankenhaus.

Ein Teil dieses Datenschutzes ist auch die Anonymisierung und Kodifizierung von medizinischen Daten für die Forschung. Wie erwähnt, sind international verknüpfte Daten eine der großen Trumpfkarten für unseren Kampf gegen die Pandemie. Hier gilt es, sicherzustellen, dass Daten keine Rückschlüsse auf die Person dahinter zulassen. Damit können sie in der Forschung sicher eingesetzt werden und eine Basis für wissenschaftliche Weiterentwicklung liefern. Vor allem die Politik sollte deutlich unterstreichen, dass Big Data auf dem Prinzip der Anonymisierung und Verschlüsselung basiert. Die Wissenschaft interessiert sich nicht für das Individuum. Wissenschaftler müssen einfach wissen und feststellen dürfen, welche inhaltlichen Verknüpfungen es gibt. Wer Cluster identifizieren will, muss wissen, welche Daten zu verarbeiten sind.

Wünschenswert wäre hier etwa ein zentrales Archiv, das staatlich verwaltet wird und in dem der Staat auch haftungs- und datenschutzrechtlich die Verantwortung übernimmt. Vorbild könnte hier das finnische Modell sein, in dem schon lange sowohl die medizinische Forschung als auch die IT zusammenarbeiten und beide gleichermaßen voneinander lernen und profitieren. Schließlich ist es nur folgerichtig, wenn öffentlich erhobene Daten der öffentlichen Forschung zur Verfügung gestellt werden. Der Zugang zu diesen wertvollen Daten ist entscheidend für die Forschung und innovative Ergebnisse. Nicht minder entscheidend ist aber auch, wie erwähnt, das Thema Datenschutz

Statement Dr. Amann

Für viele von uns ist das Heim während der Krise zum Büro geworden, und auch viele andere Aspekte unseres Lebens sind verstärkt „online“ gegangen. Leider trifft das auch für Kriminelle zu, die ihren Fokus in dieser Zeit der Heimarbeit verstärkt auf die Cyberkriminalität gerichtet und hier vor allem auch den Gesundheitssektor als ein lohnendes Ziel entdeckt haben. Das verursacht nicht nur enorme wirtschaftliche Schäden, sondern kann auch reale Auswirkungen auf die Gesundheitsversorgung haben.

So haben Kriminelle das allgemeine Interesse der Öffentlichkeit hinsichtlich der COVID-19-Krise rasch missbraucht, um Phishing-E-Mails zu verbreiten, um mit neuen Betrugsmaschen basierend auf der Krise Geld zu machen oder Websites aufzusetzen, um gefälschte oder minderwertige Produkte wie Gesichtsmasken, Corona-Testkits oder Arzneimittel zu verkaufen. Der Vertrieb dieser Arten von gefälschten oder minderwertigen Produkten gefährdet unsere Gesundheit und Sicherheit bei gleichzeitiger Erzielung erheblicher illegaler Gewinne für Kriminelle.

Darüber hinaus haben sich aber vor allem Ransomware-Angriffe als ernstes Risiko für den Gesundheitssektor entwickelt. Dabei handelt es sich um Schadsoftware, welche Computer und andere elektronische Geräte befällt und die Daten, die darauf gespeichert sind, verschlüsselt. Der Betroffene wird dann aufgefordert, Lösegeld, meist in einer Kryptowährung wie Bitcoin, zu bezahlen. Es wurden mehrere solcher Angriffe gemeldet, die eine große Anzahl von Unternehmen im Gesundheitssektor betreffen. Neben der Verschlüsslung der Daten sind einige Kriminelle mittlerweile auch dazu übergegangen, den Betroffenen mit der Veröffentlichung der gestohlenen Daten zu drohen, um so weiter Druck für die Bezahlung der Lösegeldforderung zu erzeugen. Auch wenn es grundsätzlich nachvollziehbar ist, warum einige Unternehmen in solchen Fällen bereit sind, den Forderungen nachzugeben, ist die Empfehlung aus polizeilicher Sicher ganz klar: Bitte zahlen Sie nicht! Zum einen, weil man damit das kriminelle Geschäftsmodell Ransomware weiter befeuert und unter Umständen andere Verbrechensformen mitfinanziert, zum anderen, weil überhaupt nicht gesichert ist, ob man bei einer Zahlung seine Daten zurückbekommt. Man verlässt sich schließlich bei einer Zahlung auf die Ehrlichkeit von Kriminellen. Darüber hinaus erhöht man bei einer Bezahlung das Risiko, wieder Ziel eines Angriffes zu werden, da sich Kriminelle die ‚Zahlungswilligkeit‘ eines betroffenen Opfers merken. Stattdessen empfehle ich, die Ermittlungsbehörden zu kontaktieren.

Neben Ransomware-Angriffen spielen auch DDoS (*Distributed Denial of Service*)-Attacken, wo die Nichtverfügbarkeit eines Dienstes oder Servers über eine große Anzahl von Anfragen gezielt herbeigeführt wird, sowie „Fake-News“-Kampagnen eine Rolle - mit potenziell schädlichen Folgen für die öffentliche Gesundheit und effektiver Krisenkommunikation.

Angetrieben wird das durch eine fortschreitende Industrialisierung der Cyberkriminalität - dem *Crime-as-a-Service*-Modell. Kommerzielle Anbieter verkaufen das benötigte Wissen sowie die notwendigen Werkzeuge und Dienste vom primären Angriff bis hin zur Geldwäsche. Während cyber-kriminelle Aktionen früher oft relativ kostspielig waren und solche Aktivitäten im Regelfall auch über die technischen Kapazitäten von traditionellen Kriminellen hinausgingen, ist mittlerweile ein Markt für illegale digitale Dienste und Leistungen gewachsen und gereift, der zu einer gewinnorientierten Industrialisierung der Cyberkriminalität geführt hat. Dazu gehört

unter anderem das *Ransomware-as-a-Service* Modell, wo die Verschlüsslungs-Schadsoftware quasi als Service von Kriminellen gekauft werden kann.

Neben der Industrialisierung und Kommerzialisierung der Cyberkriminalität sind es vor allem die wachsende Anzahl an mit dem Internet verbundenen Geräten – das Internet der Dinge – und die daraus resultierende Komplexität, gepaart mit unzureichenden oder nicht vorhandenen Sicherheitsmaßnahmen, die Kriminellen immer mehr Angriffsmöglichkeiten bieten. Im Gesundheitsbereich spielt hier vor allem das medizinische Internet der Dinge eine Rolle, wo Angriffe mittlerweile nicht mehr nur über normale Computer erfolgen können, sondern auch über medizinische Geräte, welche mit dem Internet verbunden sind.

Die steigende Bedrohung durch Ransomware verdeutlicht beispielhaft die Notwendigkeit, Cybersicherheit als ein umfassendes Konzept zu begreifen, welches nicht nur die IT-Dimension und somit auch alle medizinischen Geräte beinhaltet, sondern auch alle Prozesse und Mitarbeiter umfasst. Cyberangriffe wie Ransomware-Attacken können jeden treffen, natürlich auch Krankenhäuser, Labors und niedergelassene Ärzte. Da ist es unumgänglich, auf Cyberbedrohungen organisatorisch vorbereitet zu sein. Das bedeutet, dass man sowohl die technischen als auch die organisatorischen Mittel, Möglichkeiten, Prozesse, und Werkzeuge zur Verfügung hat, um adäquat auf Cyberangriffe reagieren zu können. Neben technischen Maßnahmen gehören dazu natürlich auch die kontinuierliche Fortbildung und Sensibilisierung der Mitarbeiter, um das „menschliche Betriebssystem“ adäquat abzusichern.

Ich empfehle einen proaktiven Ansatz, der über Bewusstseinsbildung, Mitarbeiterschulung, dem Umsetzen geeigneter Sicherheitsmaßnahmen wie zum Beispiel einer geeigneten Backupstrategie für die Daten bis hin zum Erstellen von Notfallplänen für den Fall der Fälle reicht. Ein kooperativer Ansatz in Zusammenarbeit mit Industrie und nationalen Ermittlungsbehörden ist dabei unumgänglich. So hat zum Beispiel das BVT in den letzten zwei Jahren regelmäßig Workshops mit dem Titel „Schützenswertes Krankenhaus“ mit den diversen Krankenhausträgern veranstaltet, wo das Thema Cybersicherheit und die diesbezügliche Bewusstseinsbildung ein wesentlicher Bestandteil waren. Die Workshop-Reihe war im Jahr 2019 für den österreichischen Sicherheitspreis nominiert und wurde unter die Top 3 gewählt. Leider hat die Krise die Workshop-Reihe unterbrochen, weitere Events sollen jedoch spätestens ab dem Jahr 2021 wieder stattfinden.

Die Bekämpfung der Cyberkriminalität ist natürlich ein Schwerpunkt der kriminalpolizeilichen Arbeit in Österreich. Dazu wurde eigens eine Meldestelle eingerichtet, die Ihnen rund um die Uhr und zwar 24 Stunden, 7 Tage die Woche Auskunft gibt. Wenn Sie Opfer von Cyberkriminalität geworden sind oder einen Verdachtsmoment haben und über die weitere Vorgangsweise Informationen benötigen, wenden Sie sich bitte an das Bundeskriminalamt unter against-cybercrime@bmi.gv.at. Nur gemeinsam können wir erfolgreich sein!

Zuletzt möchte ich auch noch besonders unsere Initiative „No More Ransom“ (https://www.nomoreransom.org/) hervorheben. Dabei handelt es sich um eine erfolgreiche Kooperation mit der Privatindustrie, wo wir konkrete Hilfe anbieten können mit zurzeit mehr als 100 frei zur Verfügung stehenden Werkzeugen, mit denen sich mehr als 140 Ransomware-Familien entschlüsseln lassen.

Statement Dr. Granig

Gesundheitsbezogene Daten werden heute an vielen Stellen – nicht nur im Gesundheitssektor – elektronisch gespeichert. Kriminelle finden aufgrund schlechter Cyber Security vielfältige Möglichkeiten vor, diese zu stehlen.

Im Gegensatz zum Finanzbereich, wo in vielen Fällen eine Schadenswiedergutmachung möglich ist (beispielsweise können entwendete Geldbeträge von Banken an Geschädigte rückerstattet werden), ist die Vertraulichkeit von Gesundheitsdaten, die unwillentlich öffentlich gemacht werden, für immer verloren. Betroffene können dafür zwar einen Schadenersatz erhalten, die Veröffentlichung kann allerdings nicht mehr ungeschehen gemacht werden. Dabei kann das ungewollte Bekanntwerden von Gesundheitsdaten erhebliche Auswirkungen und unerwünschte Folgen im sozialen oder beruflichen Kontext der Betroffenen haben. Sollte ein Angreifer überdies in der Lage sein, Gesundheitsdaten zu manipulieren, könnte er wesentlichen Einfluss auf Therapieentscheidungen und auf die Gesundheit von Patienten haben.

Cyberkriminelle nutzen für ihre Angriffe menschliche und technische Schwachstellen aus. Sie hacken sich in jahrzehntealte Krankenhausinformationssysteme oder in spezielle medizinische Geräte. Früher waren diese häufig ohne Netzwerkverbindung aufgestellt, hatten eine spezielle, sehr sichere Software und keine Schnittstelle nach außen. Heute hängen viele dieser Geräte am Netzwerk und nutzen Standard-Betriebssysteme und Standard-Schnittstellen für Datentransfers, über die Kriminelle Daten über die Patienten und deren Behandlung erlangen können.

Mit fortschreitender Digitalisierung und der Verfügbarkeit hoher Bandbreiten ist es möglich, riesige Datenbestände in kurzer Zeit zu stehlen und zu durchsuchen, wenn diese nicht verschlüsselt abgelegt sind. Das gilt vor allem auch für Innentäter bei Gesundheitsdienste-Anbietern, die auf Memory Sticks große Datenmengen unbemerkt kopieren können.

Gesundheitsdaten können auf vielfältige Art und Weise für Straftaten verwendet werden:

- Kranke können erpresst werden (z.B. Politiker mit Depressionen, Frauen, die Abtreibungen vorgenommen haben, Menschen mit schweren chronischen Erkrankungen, die stigmatisiert sind).
- Daten können manipuliert werden, um Betroffenen eine Krankheit (z.B. mittels eines gefälschten Laborergebnisses) oder ein falsches Ergebnis (etwa bei Vaterschaftstests) vorzutäuschen.
- Betreiber von Gesundheitssystemen können mit der Veröffentlichung von Datenlecks erpresst werden, da dies ihre Reputation nachhaltig schädigen würde.

Ein relativ neues, aber sehr wichtiges Feld ist auch der Bereich der mobilen Gesundheits-Apps. Solche Anwendungen speichern sensible und persönliche Daten, von der Pulsfrequenz, über Aufzeichnungen des Schlafrhythmus bis hin zu ärztlichen Verordnungen oder Informationen über Erkrankungen. Ein gestohlenes und danach gehacktes Smartphone kann somit sehr viele Informationen über den Gesundheitszustand des Nutzers preisgeben.

Neben der laufenden Überprüfung der technischen Rahmenbedingungen sind gute Sicherheitsprozesse unabdingbar für den Kampf gegen Datenlecks und Angriffe: So sollten etwa sensible Gesundheitsdaten nicht irrtümlich und unverschlüsselt an eine falsche Adresse versandt werden können. Und überdies sollten die Mitarbeiter laufend vor den Gefahren von

Spam-Mails gewarnt werden, damit auf diesem Weg eine Organisation nicht von Ransomware befallen wird und – im Falle ungenügender Backups – nicht mehr arbeiten kann.

Daher ist es sehr wichtig, dass Anbieter von Gesundheitsdiensten eine regelmäßige Überprüfung der Sicherheit ihrer Computersysteme, Applikationen und Sicherheitsprozesse durchführen und ihre Systeme modernisieren.

Wer jetzt in verbesserte Cybersicherheit und in die IT-Infrastruktur investiert, hat die Möglichkeit, im Rahmen der neuen, staatlichen Investitionsprämie 14% Förderung zu erhalten. Die bis Ende Februar 2021 angebotene Investitionsprämie ist ein Anreiz, bereits geplante oder neue Digitalisierungsprojekte umzusetzen.

Grant Thornton hat mit dem „Cyber Security Health Check“ einen Online-Fragebogen entwickelt, der eine unentgeltliche Möglichkeit darstellt, um in wenigen Minuten eine grobe Übersicht über die aktuelle Sicherheitssituation zu bekommen:

- Wie ausgeprägt ist das Sicherheitsbewusstsein?
- Wie sicher wird das Internet genutzt?
- Wie sicher sind IT-Strategie und IT-Architektur?
- Gibt es ein internes Kontrollsystem zur Bewertung von Risiken?
- Wie ausgeprägt ist der Datenschutz?
- Welche Sicherheitsvorkehrungen und Notfallprozesse gibt es?
- Werden mobile Applikationen eingesetzt, die mit sensiblen Daten arbeiten?
- Wie sieht es mit der physischen Sicherheit für die Systeme aus?

Der Cyber Security Health Check von Grant Thornton Austria ist abrufbar unter www.cyberhealthcheck.at.