

„Nicht ob, sondern wann“

Cyberkriminelle haben es auch auf Praxen abgesehen

Auf 223 Milliarden Euro schätzen Experten die Schäden, die durch Cyberkriminelle 2021 verursacht wurden – Tendenz stark steigend. Auch Arzt- und Zahnarztpraxen rücken zunehmend ins Visier internationaler Hackerbanden. Ende April hielt der Präsident des Bayerischen Landeskriminalamts (BLKA) Harald Pickert einen spannenden Vortrag im Zahnärzthehaus München, bei dem die Teilnehmer auch erfuhren, wie man sich vor Angriffen schützen kann.



Hoher Besuch im Zahnärzthehaus München: Kriminalhauptkommissar Andreas Nath und BLKA-Präsident Harald Pickert (1. Reihe, Mitte) referierten über das Thema „Cybercrime – Wie gefährdet ist Deutschland?“. Begrüßt wurden die beiden von den Bezirksstellenvorsitzenden München und Oberbayern sowie vom Vorstand der KZVB.

„Die Frage ist nicht ob, sondern wann man zum Ziel einer Hackerattacke wird“, schrieb der BLKA-Präsident den Teilnehmern gleich zu Beginn ins Stammbuch. So gaben 88 Prozent der deutschen Unternehmen bei einer Bitkom-Studie an, dass sie im Jahr 2021 von Industriespionage oder Sabotage betroffen waren. Die restlichen zwölf Prozent vermuten es zumindest. Im Jahr 2017 waren dagegen nur 53 Prozent betroffen. Auch 47 Arzt- und fünf Zahnarztpraxen waren 2021 Opfer von Cybercrime. Dieser Begriff wird im Polizeijargon immer dann verwendet, wenn das Internet die „Tatwaffe“ ist. Die größte Gefahr geht derzeit von sogenannter Ransomware aus, also Schadsoftware, die in die Praxis-IT

eingeschleust wird und oft monatelang unbemerkt bleibt.

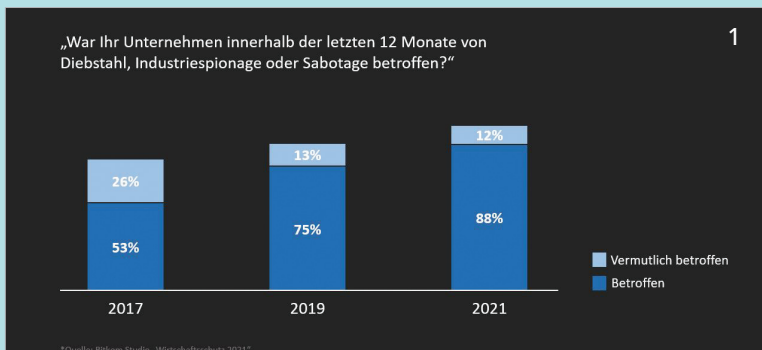
Daten werden verschlüsselt

Kriminalhauptkommissar Andreas Nath schilderte den Fall einer Arztpraxis, die eine Einladung zu einem „Teams“-Meeting bekam. Eine arglose Mitarbeiterin klickte auf den beigegefügt Link und danach standen den Hackern buchstäblich alle Türen offen. Die Schadsoftware saugte nach und nach den gesamten Datenbestand der Praxis ab und verschlüsselte ihn. Kurz darauf erhielt der Arzt eine Lösegeldforderung. Folgende Faktoren erleichtern Nath zufolge den Kriminellen ihre Aktivitäten: organisatorische Mängel,

technische Mängel und vor allem auch menschliches Fehlverhalten. Der Kommissar riet den Zahnärzten dringend dazu, neben einem IT-Basischutz auch ein IT-Sicherheitskonzept zu entwickeln sowie bei den Mitarbeitern ein Bewusstsein für die Bedrohungen aus dem Netz zu schaffen. Wissenslücken, Neugierde, Autoritätsrespekt und unsichere Passwörter erleichterten Cyberkriminellen ihr Geschäft. Gerade das Gesundheitswesen sei für die Täter attraktiv. So würden Daten nicht nur verschlüsselt, sondern auch veröffentlicht. Der Imageschaden für die Betroffenen sei enorm. Dies erkläre auch die hohe Dunkelziffer bei derartigen Attacken. Viele Unternehmen würden aus Angst um ihren Ruf keine Anzeige erstatten. Doch das sei genau der falsche Weg. Das Landeskriminalamt sei in Bayern der richtige Ansprechpartner für Cybercrime-Delikte. „Wir unterstützen bei der Wiederherstellung der Daten und arbeiten mit Polizeibehörden im Ausland zusammen“, so Nath. Außerdem gebe es eine Zentralstelle Cybercrime bei der Generalstaatsanwaltschaft in Bamberg. Die Ermittlung der Täter sei zwar schwierig, gerade wenn sie sich im Ausland aufhielten, dennoch gebe es immer wieder Fahndungserfolge. „Je mehr Delikte zur Anzeige gebracht werden, desto mehr Täter können wir überführen“, meinte BLKA-Präsident Pickert.

TI schafft neue Risiken

Organisiert wurde die Veranstaltung von den KZVB-Bezirksstellen München und Oberbayern. Dr. Michael Gleau, Bezirksstellenvorsitzender in Oberbayern, nutzte die Gelegenheit, um auf die Risiken im Zusammenhang mit der Telematik-Infrastruktur (TI) hinzuweisen. „Auch im Ge-



2

9 von 10 Unternehmen waren 2020/2021 betroffen

Nicht „ob“ sondern „wann“!

Quelle: Bitkom Studie „Wirtschaftsschutz 2021“

3

Zentrale Ansprechstelle Cybercrime

ZAC

Telefon +49 89 1212 3300
zac@polizei.bayern.de

© Bayerisches Landeskriminalamt

sundheitswesen häufen sich die Angriffe internationaler Hackerbanden. In Singapur, Schweden und vielen anderen Ländern, die weiter digitalisiert sind als wir, wurden hochsensible Patientendaten im Internet veröffentlicht.

Ungeachtet dessen treibt der Gesetzgeber die Digitalisierung unseres Gesundheitswesens weiter voran – auch mit Zwangsmaßnahmen. Doch wie so oft, schießt die Politik über das Ziel hinaus. Die Vernetzung des gesamten deutschen Gesundheitswesens ist eine Herkulesaufgabe, an der man nur scheitern kann. Macht es wirklich Sinn, dass der Zahnarzt in München auf Befunde einer Klinik in Hamburg zugreifen kann? Genau das wäre aber das Wunschdenken der gematik. Alles soll für alle zugänglich sein; und damit natürlich auch für Unbefugte, wenn sie über ausreichend kriminelle Energie und die entsprechenden technischen Fähigkeiten verfügen. Die Zahnärzte sind nicht gegen die Digitalisierung. Wir setzen in unseren Praxen schon lange auf digitale Technik. Digitales Röntgen, eine elektronische Patientenkartei, Intraoralkameras und die digitale Abdrucknahme – das setzen wir schon heute ein. Wir sind aber gegen eine Digitalisierung, die nur Selbstzweck ist und für uns Zahnärzte keinen Mehrwert mit sich bringt. Die elektronische Patientenakte ist für uns so wie die gesamte Telematik-Infrastruktur zuallererst mit zusätzlichem Aufwand ohne irgendeinen Nutzen verbunden“, so Gleau. Er warnte davor, die Gesundheitsdaten von über 70 Millionen gesetzlich versicherten Patienten zentral zu speichern. Die elektronische Patientenakte sei in ihrer jetzigen Form geradezu eine Einladung an die internationale Hackerszene. Auch Pharmaunternehmen seien sicher dankbar, wenn sie keine umfangreichen Studien zur Wirksamkeit von Medikamenten mehr bräuchten. Die elektronische Patientenakte (ePA) liefere die gewünschten Daten per Mausklick. „Ich vermiss eine gesamtgesellschaftliche Diskussion darüber, was wo gespeichert wird und wer darauf Zugriff hat. Gerade vor den zunehmenden Aktivitäten der internationalen Hackerszene muss die Politik Antworten auf diese Fragen geben“, so Gleau.

Leo Hofmeier

Abb 1: Cyberkriminalität nimmt von Jahr zu Jahr zu. – Abb 2: „Die Frage ist nicht ob, sondern wann man davon betroffen ist“, meinte der BLKA-Präsident. – Abb. 3: Zentrale Ansprechstelle: Betroffene sollten sich in Bayern an das Landeskriminalamt wenden, das ein eigenes Dezernat Cybercrime eingerichtet hat.