Wegen fahrlässiger Tötung vor Gericht

Viechtach. (job) Wegen fahrlässiger Tötung verantworten musste sich ein Pfleger am Mittwoch vor dem Amtsgericht Viechtach (Kreis Regen). Dem Vorwurf, durch eine Pflichtverletzung den Tod eines Patienten verursacht zu haben, widersprach er vehement. Vielmehr nannte er ein Kommunikationsproblem zwischen ihm und seiner Kollegin als Ursache für den Unfall. Diese habe den Personenlift, mit dem der junge Mann vom Bett in einen Rollstuhl gesetzt werden sollte, ohne seine Freigabe und die erneute Kontrolle der Gurte bewegt, sagte der Angeklagte aus. Die Verhandlung wird Mitte April fortgesetzt. Dann kann sich auch die Kollegin zu dem Unglücksfall äußern, falls sie als Zeugin Angaben machen möchte. Einen ausführlichen Bericht lesen Sie in einem Teil der Auflage.

Medizincampus: Hausärzte unzufrieden

Regensburg/München. (red) Bayerns Hausärzteverband begrüßt die Entscheidung der Bayerischen Staatsregierung, in Niederbayern einen Medizincampus mit bis zu 600 Studienplätzen zu schaffen. „Jeder einzelne Studienplatz hilft“, kommentiert Markus Beier, Landesvorsitzender des Bayerischen Hausärzteverbandes, die Bekanntgabe des Ministerrates vom Dienstag.

Umso unverständlicher sei es allerdings, dass die Universität Regensburg, zu der der Medizincampus Niederbayern gehören wird, als einzige Hochschule in Bayern noch immer keinen eigenen ordentlichen Lehrstuhl für Allgemeinmedizin habe, hieß es in einer Mitteilung von Mittwoch. Doch gerade diese sei wichtig, um dem Verwaisen der Hausarztpraxen auf dem Land entgegenzuwirken.

„Diese Negativspirale können wir nur stoppen, wenn wir die Medizinstudierenden frühzeitig für die Allgemeinmedizin begeistern. Alle anderen Universitäten in Bayern haben das bereits erkannt und eigene ordentliche Lehrstühle für Allgemeinmedizin eingerichtet. Nur die Universität Regensburg ist hier Schlusslicht“, sagte der Landesvorsitzende Markus Beier.

Coronavirus in Ostbayern

Die 7-Tage-Inzidenz entspricht der Anzahl der in den letzten sieben Tagen neu gemeldeten Fälle pro 100.000 Einwohner.

Landkreis/Stadt	7-Tage-Inzidenz	Wert Vortag
Deggendorf	2508,4	2404,6
Dingolfing-Landau	2631,5	2367,2
Freyung-Grafenau	2362,3	2349,6
Kelheim	2678,5	2708,5
Landshut	2651,5	2361,2
Landshut Stadt	2077,6	1907,9
Passau	2741,2	3195,6
Passau Stadt	2394,4	2134,9
Regen	2552,0	2546,8
Rottal-Inn	2544,3	2458,1
Straubing Stadt	1172,0	1180,4
Straubing-Bogen	1498,8	1415,3
Amberg Stadt	1486,3	1426,8
Amberg-Sulzbach	1835,0	1822,4
Cham	3062,6	3104,8
Neumarkt	84,3	154,6
Neustadt/Waldnaab	2718,6	2667,9
Regensburg	2495,9	2914,9
Regensburg Stadt	2441,7	2789,8
Schwandorf	1600,2	1545,0
Tirschenreuth	2546,9	2619,4
Weiden Stadt	2412,1	2355,7
Gesamt Bayern	2183,4	2185,9

Rote Zahlen stellen steigende, blaue Zahlen fallende und schwarze Zahlen gleichbleibende Inzidenzen dar.

Stand: 23.03.2022 / Quelle: Robert-Koch-Institut

„Dingolfing wird kein Einzelfall bleiben“

Ein IT-Sicherheitsexperte erklärt, wie sich Kommunen vor Cyberangriffe schützen können

Ein Trojaner legt die Stadtverwaltung Dingolfing lahm. Nach dem Cyberangriff, der am vergangenen Wochenende entdeckt wurde, waren sämtliche Festplatten im Rathaus verschlüsselt. Ob nicht nur die Zugriffe blockiert, sondern auch sensible Daten abgegriffen wurden, muss nun geklärt werden. Die Höhe des Schadens? Noch unklar. IT-Sicherheitsexperte Bernhard Altschäffel aus Aiterhofen (Kreis Straubing-Bogen) warnte zuletzt immer wieder davor, dass sich der Ausbau der Digitalisierung – Stichwort Homeoffice – nicht nur für Unternehmen, sondern auch für Kommunen zu einem Stresstest entwickelt hat, und Sicherheitsvorfälle weiter zunehmen werden.

Bernhard Altschäffel ist anerkannter Berater und IT-Sicherheitsexperte. Foto: Photography Sascha Iwanow

Herr Altschäffel, erklären Sie mal, was ein Trojaner ist und was er im Rathaus Dingolfing angerichtet hat.

Bernhard Altschäffel: Der Name „Trojaner“ leitet sich tatsächlich vom Trojanischen Pferd in der Mythologie ab: Getarnt als nützliche Anwendung wird ein Programm in fremde IT-Systeme eingeschleust, um dort heimlich andere, unerwünschte Funktionen auszuführen. Bis der Trojaner vom Nutzer bemerkt oder von der IT-Security aufgespürt wird, hat er seine feindliche Mission oft schon erfüllt und eigenständige Schadprogramme, wie Spionagesysteme oder Verschlüsselungssysteme (Spyware und Ransomeware, Anm. d. Red.) installiert. Letztlich zielen die Angriffe darauf ab, Daten und Informationen zu stehlen sowie das System zu kontrollieren oder zu beschädigen.

Lassen sich Cyber-Angriffe wie auf das Rathaus Dingolfing überhaupt verhindern?

Altschäffel: Den Cyber-Angriff, auf den man sich dann sozusagen optimal vorbereiten könnte, gibt es leider nicht. Cyberkriminalität ist zum professionell-organisierten Industriezweig geworden, der seine Methoden und Technologien kontinuierlich optimiert. Jedes Unternehmen und jede Behörde ist Ziel von Cyberangriffen, die Frage ist, ob sie auch Opfer von solchen Attacken werden. Unsere Gegner sind Profis – und es gibt kein IT-Netz, das nicht irgendwann gehacked werden kann. Aber Behörden und Unternehmen stehen dem nicht machtlos gegenüber: Sie können ein Sicherheitssystem schaffen, das Attacken erschwert und damit unattraktiver macht, das erfolgreiche Angriffe schnell erkennt und das kritische Daten besonders schützt.

Nehmen Cyberangriffe zu oder sichern sich Unternehmen und Verwaltungen nur zu wenig ab?

Altschäffel: Cyberangriffe nehmen seit Jahren kontinuierlich zu. Laut dem Branchenverband Bitkom hat sich die Schadenssumme in Deutschland vom Vergleichszeitraum 2018-2019 auf 2020–2021 verdoppelt: von 103 auf 220 Milliarden Euro. Kommunen geht es da nicht anders als allen anderen Unternehmen. Sie sind für Cyberangreifer lohnende Ziele, denn Städte und Gemeinden verarbeiten sensible, personengebundene Daten. Die Bereitschaft, Lösegeld im Falle eines Ransomware-Angriffs zu zahlen, wird daher voraussichtlich sehr groß sein. Und die Verwaltungen stehen dabei natürlich im besonderen Fokus der Öffentlichkeit: Die Bürger erwarten, sicher auch zu Recht, dass ihre persönlichen Daten geschützt sind. Kurz gesagt: Ein Datenleck in den Kommunen darf es nicht geben.

Welche Fehler machen Unternehmen und Kommunen in Hinblick auf IT-Sicherheit am häufigsten?

Altschäffel: Informationssicherheit ist leider kein einmal zu erreichender Dauer-Status, sondern ein stetes Wettrennen, ein Dauerlauf, wenn man so will: Digitale Grundfitness sowie die richtige Ausstattung sind die Voraussetzungen. Dann sollte man sich den Weg überlegen und diesen dann regelmäßig überprüfen. Das mögen schweißtreibende Aussichten sein, aber es ist die Herausforderung, der wir uns stellen müssen und können. Ich würde es so sagen: Nur gemeinsam kann Sicherheit geschaffen werden. Gefragt sind hier vor allem die Führungskräfte in Kommunen und Unternehmen: IT- und Datensicherheit braucht die nötige Aufmerksamkeit und Gewichtung.

„Pandemie war und ist Stresstest für IT-Sicherheit“

Vielen denken wohl, sie sind zu unbedeutend für Cyber-Attacken ...

Altschäffel: Wir betreuen viele Unternehmen, die zunächst meinten, dass ihre Daten gar nicht interessant genug sind, um gestohlen zu werden. Entscheidend ist aber die Frage, wie wertvoll sind meine Daten für mich. Und wie lange kann ich ohne meine Daten und meine IT überleben?

Wie sehr haben sich IT-Sicherheitsprobleme mit der zunehmenden Digitalisierung während der Pandemie verstärkt? Wo sehen Sie die gravierendsten Lücken?

Altschäffel: Die Pandemie war und ist ein Stresstest für die IT-Sicherheit: Homeoffice-Infrastrukturen mussten unter Zeitdruck aufgebaut werden und gleichzeitig galt es, den Arbeitnehmern im Homeoffice bewusstzumachen, dass sie gerade daheim, fernab vom geschützten Unternehmensnetz, verantwortungsvoll mit Daten umgehen müssen.

Wo lauern die konkreten Gefahren, wenn die Mitarbeiter im Homeoffice sitzen?

Altschäffel: Nicht selten tummeln sich zu Hause im selben Netzwerk oder in derselben physischen Umgebung andere User wie Familienmitglieder, die nicht das gleiche Sicherheitsbedürfnis haben. Dazu kommt die allzu menschliche Tendenz, sich daheim lockerer und legerer zu verhalten. Heimarbeitsplätze sind eine Riesenherausforderung für Unternehmen und deren IT-Abteilungen. Darüber wird in den nächsten Jahren noch viel zu lesen sein. Ich oute mich hier gerne als Homeoffice-Hiob, denn momentan werden viele der damit einhergehenden Sicherheitslücken von den akuten Anforderungen überlagert oder auch einfach verschwiegen.

Wie schützen Sie als Fachmann Daten in Ihrem Unternehmen, aber auch privat, wenn Sie von Zuhause arbeiten?

Altschäffel: Nun, privat bin ich, das gebe ich offen zu, oft etwas nachlässig. Natürlich nutze ich ein jeweils aktuelles Antivirus-Programm und führe auch regelmäßig die empfohlenen Updates durch. In Sachen Datensicherung bin ich etwas laxer unterwegs und sichere mein System nur alle zwei bis drei Wochen. Das Wichtigste aber: Ich trenne mein privates System strikt von meinen Arbeitsrechnern. Das mag manchmal etwas unkomfortabel sein, aber das Risiko, mit privaten Anwendungen mein Unternehmensnetz zu infizieren, ist mir einfach zu groß.

Man kann also nicht vorsichtig genug sein ...

Altschäffel: „Team Vorsicht“ alleine hilft da nicht. Ich nenne es gerne „Team TOM“, Technik-Organisation-Mitarbeiter. Aktuellste Technik beziehungsweise Tools einsetzen, organisatorische Voraussetzungen schaffen und alle Mitarbeiter explizit und aktiv einbinden. Mitarbeitende sind und bleiben die wichtigsten Schutzschilder oder Risikofaktoren in der IT.

Welche Lehren sollte man in Dingolfing, aber auch in anderen Kommunen nach einer Cyberattacke unbedingt ziehen?

Altschäffel: Das kann ich nicht beantworten, da ich weder den konkreten Ablauf noch die betroffene IT-Infrastruktur kenne. Der Fall Dingolfing zeigt: Alle Unternehmen und Kommunen sind im Visier von Cyberangriffen, sei es als bewusst ausgesuchtes oder als zufälliges Angriffsziel. Dingolfing wird daher, auch bei uns in der Region, kein Einzelfall bleiben. Mein Appell: Egal ob CEO oder Bürgermeister, IT- und Datensicherheit muss Chefsache sein. Die Fachkräfte müssen mit den notwendigen Werkzeugen ausgestattet werden, die Mitarbeitenden müssen sensibilisiert werden und für den Fall der Fälle sollte eine Versicherung abgeschlossen werden. Letzteres hat schon manchen vor dem Ruin bewahrt.

Interview: Ingmar Schweder

ZUM THEMA

Drei Empfehlungen für mehr IT-Sicherheit im Unternehmen vom IT-Berater Bernhard Altschäffel:

› **Schaffen Sie** ein Bewusstsein für IT-Sicherheit bei Ihren Mitarbeitenden. Sicherheit ist nicht sexy, aber Menschen sind und bleiben der größte Risikofaktor, der häufigste „Türöffner“ für Cyberattacken.

› **Suchen Sie** sich einen hochprofessionellen IT-Partner. Wir haben unsere IT an einen deutschen Cloud-Service-Provider ausgelagert, der sämtliche Updates und Datensicherungen automatisiert durchführt.

› **Versichern Sie** Ihre Cyberrisiken, inklusive möglicher Schäden durch Betriebsunterbrechungen. Das verhindert keinen Angriff, lässt Sie aber ruhiger schlafen. (is)